CG | फिन्को
विश्वसनीयताको अनुभूति

Version 3.0

# AML/CFT POLICY AND PROCEDURES

# of

# CG FINCO LIMITED

# 2023

Under the umbrella of
Chaudhary Group - Nepal
(Financial Services/Remittance Division)

CG CHAUDHARY® GROUP
*Touching life everyday*

# Version Control

| Version | Date | Description of changes |
|---|---|---|
| **1.0** | November 12, 2017 | First issued version “KYC and AML policy of CGFL 2017” is reviewed and approved by Chairman |
| **2.0** | August 25, 2022 | Policy named as AML/CFT policy & procedures of CG Finco Ltd 2022 |
| | | “Frauds and its preventions" has been added on section B |
| | | Updated/corrections |
| **3.0** | November 21, 2023 | “Threshold transactions (No. 20) & Political Exposed Persons (No. 28)” has been added on section A |
| | | Updated/corrections |

# Table of Contents

**Particulars** **SECTION A** **Page**

# Section A

**Introduction**

This policy is named as AML/CFT policy and Procedures of CG Finco Limited (CGFL). This Policy is guided by The Assets (Money) Laundering Prevention Act, 2008 (second amendment 2070) of Nepal, Assets (Money) Laundering Prevention Rules, 2073 and Directives issued by Financial Information Unit (FIU) and Nepal Rastra Bank (NRB) & Directive on Anti Money Laundering and Combating Financing Terrorism issued by Supervision Department as well guided by Recommendation issued by Financial Action Task Force. Any change in this regards will be a part of this policy.

**Ownership**

The policy is of CG Finco Limited (CGFL)/Chaudhary Group Nepal: Financial Services/Remittance Business and has been reviewed and approved by the Board of Directors. This policy will be implemented immediately after Board Approval. As per the need, this policy will be reviewed and new policy will be implemented after obtaining approval of the Board.

**Exceptions**

No Exceptions will be entertained on AML/Compliance related matters. However, Exceptions for other issues to this policy must be approved by the Chief Compliance Officer, or a designee. All exceptions must be documented, with reasons for the exceptions, including expiration or review date and, where necessary, include an action plan and time table for Compliance with the policy.

**Scope**

This policy guideline shall apply to all CGFL's Customer Service Centers and Sub-Representatives under the network of CGFL. This policy covers the entire functional procedures to be undertaken by different departments/branches of CG Finco Limited (CGFL) from receipt of application for establishing new relationship to executing financial transactions with the Sub agents/ Customer.

**Limitation**

This policy shall not cover any changes on procedures that may arise due to changes on guidelines provided by the Nepal Rastra Bank at a later date. However, the basic parameters to analyze KYC compliance as described on the Unified Directives and circulars issued by Nepal Rastra Bank and changes from time to time must be complied with as and when the circulars are issued.

**1. Definitions**

**Know Your Customer (KYC)** is due diligence and regulation to describe the process of obtaining, retaining and using information about customer such that his/her identity and residential address is verified, the source of his/her funds and wealth is understood, his/her financial circumstances are

understood, and the nature of the transactions he/she undertakes are understood in the context of his/her known personal circumstances and activities

**Money Laundering** is the participation in any transaction that attempts to conceal or disguise the nature or origin of funds derived from illegal activities such as, fraud, corruption, tax evasion, organized crime, or terrorism etc.

**Terrorist financing** involves the solicitation, collection or provision of funds with the intention that they may be used to support terrorist acts or organizations. Funds may stem from both legal and illicit sources. The primary goal of individuals or entities involved in the financing of terrorism is therefore not necessarily to conceal the sources of the money but to conceal both the financing and the nature of the financed activity.

**Customer/sub-agent:** For the purpose of this policy, a 'Customer/sub-agent' may be defined as:

- A person or entity that maintains sub representative agreement / business relationship with CGFL.
- One, on whose behalf the remittance money is paid (i.e. the beneficial owner)

**The Policy** refers to CGFL "AML/CFT Policy and Procedures"

## 2. Objective of the Policy

The main objective of this policy is to prevent CGFL from being used, intentionally or unintentionally, by criminal elements for Money Laundering activities. Its objective is also to prevent all illegitimate financial/business transactions like concealing of identity of Business/Transaction of source of fund, Money Laundering, Terrorist financing, Drug trafficking etc. The policy also enables CGFL to know/understand its customers and their financial dealings better which will in turn help to manage its risk prudently.

Additionally, other objectives of this policy are;

a) To set procedures to identify AML/CFT transactions.

b) To make staff aware of the AML/CFT policies and practices.

c) To make aware about the consumer and agent frauds and its preventions

## 3. Money Laundering & Terrorism Financing and its policies

### 3.1 Money Laundering

Money Laundering is the attempt to conceal or disguise the nature, location, source, ownership, or control of money. Criminal activities, such as drug trafficking, smuggling, human trafficking, corruption and others, tend to generate large amounts of profits for the individuals or groups carrying out the criminal act. However, by using funds from such illicit sources, criminals risk drawing the authorities' attention to the underlying criminal activity and exposing themselves to criminal prosecution. In order to benefit freely from the proceeds of their crime, they must therefore conceal the illicit origin of these fuds.

**Stages / Process of Money Laundering**

**Placement:** Involves placing the proceeds of crime in the financial system. It refers to the physical disposal of cash, often in the form of bank deposit, through a succession of small and anonymous transactions. The money launderers insert the illicit money into a legitimate financial institution.

**Layering:** This stage involves converting the proceeds of crime into another form and creating complex nature of financial transactions to disguise the audit trails and the source and the ownership of funds (e.g. buying and selling of commodities, stocks, property etc.). It involves bank to bank transfers, wire transfers, several deposits and withdrawals, purchasing high value items etc.
**Integration:** In this stage the money re-enters the mainstream economy in the legitimate looking form. It involves placing the laundered proceeds back in the economy under the veil of legitimacy. It would be very difficult to trace the original source of the money if there is no proper documentation in the previous two stages of Money Laundering.

### 3.2 Terrorism Financing

The financing of terrorism is where funds or other property is made available, directly or indirectly, with the sole intention that the funds be used to further terrorism or to initiate terrorist acts to be carried out. The primary goal of individuals and entities involved in the financing of terrorism is therefore not necessarily to conceal the sources of the money but to conceal both the financing and the nature of the financed activity. The major source of terrorist financing includes financial support from countries, organizations or individuals that may include criminal activities and revenue generating activities, may involve drug trafficking, human smuggling, theft, robbery and fraud to generate money. Funds raised to finance terrorism usually have to be laundered and other reporting industries are important in the identification and tracking of terrorist financing activities. such transaction when detected and reported to NRB, FIU.

### 3.3 Anti-money laundering (AML) & Combating the Financing of Terrorism (CFT) Policy

AML/CFT policy serves an important function in the conduct of Remittance business. These procedures are essential to enable CGFL to perform its obligation under the International system as well as to prevent Theft, Fraud, Money Laundering and Terrorist Financing. It should be an explicit policy not to accept any Customer who cannot provide evidence of his/her identity.
Anti-money laundering (AML) policy is a term mainly used in the financial and legal industries to describe the legal controls that require financial service companies and other regulated entities to prevent detect and report money laundering activities. The Assets (Money) Laundering Prevention Act, 2008 of Nepal prohibits remittance companies be used in helping customers to conceal, transform, hide its sources or misrepresent about it.
This rule means not only to inquire about the identity of new and occasional Sub agents/Customers, but also about existing Sub agents/Customers, in particular if the CGFL find it doubtful to the customer's real identity. Such evidence shall be substantiated by reliable documents or other means. Operation In charge or Relationship Managers must confirm that Remittance transactions

are undertaken in strict adherence to policies of the CGFL. Due care should be taken to promote high ethical and professional standards and prevent CGFL from being used intentionally or unintentionally by criminal elements.

## 4. Customer Due Diligence (CDD) and KYC

**Due Diligence** is a concept involving either the performance of an investigation of a business or person or the performance of an act with a certain standard of care. The term is more commonly applied to voluntary investigation.

**Know Your Customer** is very much important to prevent theft, fraud, money laundering and terrorist financing. One aspect of KYC is to verify that the customer is not on any list of known fraudsters, Terrorists or Money launderers, Persons regarded as high risk owing to negative reports in the media/public records.

CGFL branches/Customer Service Centers & Sub-Representative office should undertake Customer Due Diligence measures, including identifying and verifying the identity of their customers, when:

a. Establishing business relations / while paying out any Transaction;
b. Carrying out occasional transactions above the applicable designated threshold
c. There is a suspicion of money laundering or terrorist financing; or
d. The company has doubts about the veracity or adequacy of previously obtained customer identification data

**The customer's due diligence measures to be taken are as follows:**

a) Identifying the customer and verifying that Customer's identity, using reliable, independent source documents, data or information.
b) Identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner such that CGFL CSC or Sub representative is satisfied that it knows who the beneficial owner is.
c) Obtaining information on the purpose and intended nature of the business relationship.
d) Conducting ongoing Due Diligence on the business relationship and scrutiny of Transactions undertaken throughout the course of that relationship to ensure that the Transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

**Situations Requiring Enhanced Due Diligence (EDD) on Customers:**

In the following certain situations, regardless of the amount transacted, CG Finco Ltd. is required to perform additional steps to conduct Enhanced Due Diligence (EDD), in addition to the CDD process being undertaken:

High Risk Customer are:

- Non-resident customers,
- High net worth individuals,

- Trusts, charities, NGOs and organizations receiving donations,
- Companies having close family shareholding or beneficial ownership,
- Firms with 'sleeping partners',
- Politically exposed persons (PEPs) of foreign origin,
- Non-face to face customers, and
- Those with dubious reputation as per public information available, etc.

**Enhanced Due Diligence (EDD) on Customers**

EDD include, but are not limited to the followings:

a. Obtain more detailed information from the customer, in particular, on the purpose of transaction and the source of funds.
b. Ask for an additional government issued IDs, even if the amount of the transaction is low.
c. Obtain approval from the senior management, such as the Business Unit Head, before establishing the business relationship or transacting with the customer.
d. When a service is provided to minor, normal identification policies must be followed along with establishing the identity of the legal parent(s) or guardian(s).
e. We will not conduct the transaction in case of non-face- to-face business as well as if the representative will act on behalf of third party.

## 5. 'Know Your Customer' Standards

The objective of 'KYC guidelines' is to prevent CGFL from being used, intentionally or unintentionally, by criminal elements for money laundering activities. KYC procedures also enable the Company to know/understand its Customers and their financial dealings better which in turn help them manage their risks prudently.

The KYC Policy of the company has been framed incorporating the following four key elements:

(i) Customer Acceptance Policy;
(ii) Customer Identification Procedures;
(iii) Monitoring of Transactions; and
(iv) Risk Management.

The CGFL should ensure that the provisions of KYC guideline of Nepal Rastra Bank, wherever applicable, are adhered to strictly.

## 6. KYC Process

### 6.1 Initiation of Relationship:

Primarily, Front Line Associate (FLA) /Operation In- charge/Regional representative / Relationship Managers or other designated staff in customer Service Center or elsewhere are responsible for interviewing the prospective customer and obtain sufficient information on the reputation of the client, legitimacy of their business and nature and source of activity expected. A business

relationship should never be established until and unless the identity of the potential Customer/Sub agent is satisfactorily established. The relation shall not be established till the potential Customer/Beneficiary provides the requested information. Likewise, if the requested follow up information is not forthcoming, the Sub Agent/Customer shall be earmarked and any further transaction shall be carried out with utmost cautiousness.

**6.2 Courteous Conduct:**

After obtaining general information and supporting documents, in the case if the FLA feels that additional information is required from the customer a ***KYC interview*** should be conducted in a very polite manner.

**6.3 Reporting:**

In case the identity of a prospective customer cannot be satisfactorily established, the refusal to establish should be conveyed to the senior body/officials and if deemed necessary a reference can be made in this regard to this policy and the instruction issued by the CGFL's Compliance department, Nepal Rastra Bank and concerned Government authorities. Recognition and reporting of suspicious transactions as follows:

- FLA must be continuously alert to unusual transactions.
- Structuring of transaction to obscure audit trail, evade identification or obstruct record keeping.
- FLA is required to report suspicious promptly, in writing to the compliance personnel who shall review the activity and determine whether a report should be made to the Nepal Rastra Bank through Compliance officer at Corporate office.
- FLA, Staff member & Sub Agent should provide the compliance officer and the person designated by him with access to all customer information within the companies possession, at his request or to the person designated by him.
- The CGFL will cooperate fully with all law enforcement activities and investigations within the scope of applicable laws and in consultation with the CGFL's legal department.
- Staff member is required to be careful not to alert, either directly and indirectly any person suspected of illegal activity or subject to a suspicious report to compliance officer.

**6.4 Questionnaire:**

The basic questionnaire for interviewing the potential customer and the required documents as part of KYC process shall be as mentioned below. However, the questions laid down in this questionnaire and the documents listed are only basic and additional information may be sought where deemed necessary. The interviewer may add or reduce the questions/document requirement depending upon the clients/customer as the case may be.

Basic documents and other requirements to establish the authenticity of the customer are listed herein below under **Annex 1.**

## 7. KYC Principles

In KYC principles, in particular when remittance payment or establishing customer relationship, the identity and relevant information of every client and related counterparties need to be obtained and studied thoroughly, to ensure that no business is conducted with money launderer, terrorist and blacklisted persons or entities.

Remittance payment or establishing new relationship, we must obtain following information. The details given below must be verified for accuracy by checking identification documents, such as Citizenship, Passport, Government Identity Cards, Driving Licenses etc.

We must not pay Remittance amount or engage in any business dealings with Customers under fictitious names or number where we do not know the original identity of the beneficiary.

In general, in the absence of any specific requirements, the following guidelines are applicable:

a) All the customers should correctly complete the relevant information in TRM form (To Receive Money Form) and furnish Identity documents as required by the rules and regulation of the Company. The copy of Identification documents of the beneficiary should be verified with the original.

b) The prospective individual Customers must establish their identities by producing /furnishing the original copy of document such as Citizenship Certificate or Passport or Driving License issued by an official authority bearing a Photograph of the holder.

c) CGFL's employee (Relationship Manager, Dealers, Operation In charge, and Customer Service Center Personnel) initiating business relationship of the company with the Customer is responsible for obtaining necessary information.

## 8. Guidelines on KYC Norms

### 8.1 Customer Acceptance Policy (CAP)

A clear Customer Acceptance Policy has been laid down with explicit criteria for acceptance of Customers. The Policy must ensure that explicit guidelines are in place on the following aspects of Customer relationship in the Company.

a) No Remittance amount is paid/No sub representative agreement is entered in anonymous or fictitious name(s);

b) Parameters of risk perception are clearly defined in terms of the location of sub representative and his clients and mode of payments;

c) Volume of turnover, social and financial status, etc. to enable categorization of sub representative into low, medium and high risk (the company may choose any suitable nomenclature, viz. level I, level II, level III etc.); sub representatives requiring very high level of monitoring, e.g. Politically Exposed Persons may, if considered necessary, be categorized even higher;

d) Documentation requirements and other information to be collected in respect of different categories of sub representatives depending on perceived risk and keeping in mind the requirements of Western Union and of NRB Guideline issued from time to time.

e) Not to pay any remittance amount or enter into any business transaction with an existing customer where the company is unable to apply appropriate customer due diligence measures, i.e. the company is unable to verify the identity and /or obtain documents required as per the risk categorization due to non-co-operation of the customer or non-reliability of the data/information furnished to the company. It may, however, be necessary to have suitable built-in safeguards to avoid harassment of the customer.

f) Necessary checks before remittance payment so as to ensure that the identity of the beneficiary does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations, etc.

g) A profile may be prepared for each new sub representatives based on risk categorization. The sub agent profile may contain information relating to the sub representative's identity, social/financial status, nature of business activity, information about his clients' business and their location, etc. The nature and extent of due diligence will depend on the risk perceived by the company. However, while preparing sub representatives profile CGFL should take care to seek only such information from the sub representatives, which is relevant to the risk category and is not intrusive. The sub representatives profile will be a confidential document and details contained therein shall not be divulged for cross selling or any other purposes.

h) Sub representatives that are likely to pose a higher than average risk to CGFL may be categorized as medium or high risk depending on sub representatives' background, nature and location of activity, country of origin, sources of funds and his client profile, etc. CGFL may apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk sub representatives, especially those for whom the sources of funds are not clear. Examples of sub representatives requiring higher due diligence (EDD) may include:

- Non-resident customers,
- High net worth individuals,
- Trusts, charities, NGOs and organizations receiving donations,
- companies having close family shareholding or beneficial ownership,
- Firms with 'sleeping partners',
- Politically exposed persons (PEPs) of foreign origin,
- Non-face to face customers, and
- Those with dubious reputation as per public information available, etc.

**8.2 Risk Perception**

No financial sector business is immune from the activities of criminal elements. The level of Money laundering Risk that CGFL is exposed to by a beneficiary/ sub representatives' relationship depends on:

- Beneficiary/type of the sub representatives
- Nature of business of sub representatives

- Type of product/service being offered by the sub representatives

Based on the above criteria, the customers are classified into three risk levels as follows:

**High Risk:**

High risk profiles include those Customers/individuals from those countries identified as 'High risk" by international agencies concerning money laundering, drug trafficking, terrorism, propensity or history of public corruption, organized crime, fraud, human rights abuses, non-existent or inadequate financial regulation, fictitious or non-recognized jurisdictions that issue fraudulent financial services licensing, and international sanction (including special measures, weak regulatory framework for alternative remittance systems, and offshore financial centers). This list also includes alerts for pseudo official or non-governmental jurisdictions or entities that issue camouflage or spurious passports.

**Medium Risk:**

Medium risk profiles include those Trust/charities /NGOs and organizations receiving donations etc.

**Low Risk:**

All the beneficiary/ sub representatives who are not high/ medium Risk customers are low risk customers. These are the type of customers whose identity and source of wealth can be easily identified e.g. salaried employees whose salary structure is well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover.

The ultimate responsibility for knowing the customer lies with the payment centers such as company's customer service center or sub representatives Offices.

**Periodical Review of Risk Categorization of Customers:**

CGFL Corporate office shall ensure maintaining and updating of sub representatives risk profile on a continuous basis. A review of risk categorization of beneficiary/ sub representatives should be carried out at a periodicity of not less than once in a year.

## 9. Customer Identification Procedure (CIP)

The KYC policy should clearly spell out the **Customer Identification Procedure** to be carried out at different stages, i.e. while establishing a relationship; carrying out a financial transaction or when the CGFL/ sub representatives has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data.

Customer identification means identifying the customer and verifying his/ her identity by using reliable, independent source documents, data or information. The CGFL and/or it's sub representatives need to obtain sufficient information necessary to establish, to their satisfaction, the identity of each new customer, whether regular or occasional and the purpose of the intended nature of relationship. Being satisfied means that CGFL &/or sub representatives must be able to

satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the prescribed guidelines in place. Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate etc.). For customers that are natural persons, the company should obtain sufficient identification data to verify the identity of the customer, his/her address/location, and also his/her recent photograph. For sub agents/customers that are legal persons or entities, the company should:

- Verify the legal status of the legal person/ entity through proper and relevant documents
- Verify that any person purporting to act on behalf of the legal person/entity is so authorized and identify and verify the identity of that person and
- Understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person.

**10. Risk Management**

The Management should ensure that an effective KYC program & AML/CFT Policy is put in place by establishing appropriate procedures and ensuring their effective implementation. The Control & Compliance Department of the CGFL shall monitor, manage and control the compliance issues of the Policies. It should cover proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility should be explicitly allocated within the company for ensuring effective implemented of KYC, AML/CFT policy. The company may, devise procedures for creating Risk Profiles of their existing and new customers and apply various Anti Money Laundering measures keeping in view the risks involved in a transaction or business relationship.

**11. Independent Audit Testing**

The Chaudhary Group Internal audit and System Cells have an important role in evaluating and ensuring adherence to the policies and procedures. As a general rule, the compliance function should provide an independent evaluation of the company own policies and procedures, including legal and regulatory requirements. Chaudhary Group Nepal should ensure that their audit machinery is staffed adequately with individuals who are well-versed in such policies and procedures. Concurrent/ Internal Auditors should specifically check and verify the application of KYC procedures & AML/CFT Policy of CGFL and comment on the lapses observed in this regard.

**12. Customer Education**

Implementation of Policies & procedures requires CGFL to demand certain information from customers which may be of personal nature or which have hitherto 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. There is, therefore, a need for the company to prepare specific literature/ pamphlets, etc. so as to educate the customer on the objectives of policies & Procedures. The Front

Line Associate (FLA) of CGFL Customer Service Center & of sub representatives' office needs to be specially trained to handle such situations while dealing with customers.

**13. Introduction of New Technologies**

Special attention should be paid to any money laundering threats that may arise from new or developing technologies including on-line transactions that might favor anonymity, and take measures, if needed, to prevent their use in money laundering schemes.

**14. KYC for the Existing Sub-agents/Regular Customers**

Due diligence should be applied to ensure effective application KYC norms to all the existing sub representatives/customers in a time bound manner. Transactions or payment process in existing sub representatives should be continuously monitored and any unusual pattern in the operation of sub representatives' business should trigger a review.

Where the CGFL or sub representative is unable to apply appropriate KYC measures due to non-furnishing of information and /or non-cooperation by the customer, the Company may consider cancel the transaction or terminating the business relationship with sub representatives after issuing due notice to the customer explaining the reasons for taking such a decision. Such decisions need to be taken at a reasonably senior level.

**15. Appointment of Compliance Officer**

The CGFL management have appointed a senior management officer to be designated as 'Compliance Officer'. Principal Officer shall be located at the Head/Corporate office of the Company and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the prescribed law. S/he will maintain close liaison with Nepal Rastra Bank, enforcement agencies, and any other institution which are involved in the fight against money laundering and combating financing of terrorism. It should also be ensured that there is proper system of fixing accountability for serious lapses and intentional circumvention of prescribed procedures and guidelines.

Further, all anti-money laundering monitoring reports made by Compliance Officer and records of consideration on those reports and of any action taken as a consequence including reporting made to management/auditors/regulators be maintained for 5 years' period for future review.

**16. Transaction Monitoring**

All the transactions will be monitored for money laundering, terrorist financing, and fraud activity as per required timely basis. Timely identification of Suspicious transaction will be reported as STR reporting under Nepal Rastra Bank, FIU Department requirements along with the implementation of transaction monitoring process and procedures.

**17. Regulatory reporting**

In the event of any suspicion, the staff concern should report the same immediately to Operation in charge/ Supervisory Manager, to ensure that there is no new fact which would negate the suspicion. If suspicion remains, the matter should be reported the compliance officer, who will review and investigate the entire case. The suspicion if well- found should be reported to the members of management. The suspicion should also be reported to Nepal Rastra Bank, FIU and/ or designated Money Laundering Law Enforcement Agencies, if any.

CGFL will ensure that their internal control system operates efficiently and cover appropriately the implementation of this regulation for Anti Money Laundering Procedures.

**18. Training**

CGFL must have an ongoing employee-training programme so that the staffs are adequately trained in Policies & procedures. Training requirements should have different focuses for frontline staff, compliance staff and staff dealing with new sub representatives. It is crucial that all those concerned fully understand the rationale behind the policies and implement them consistently.

So as to strengthen the monitoring and prevent the money laundering & terrorist financing activities an appropriate training to the employees/customers shall be provided regularly or on need basis. The training materials should be circulated to the employees/customers as per the need basis.

All the employee/customers training must be documented and reflect the name of attendees, the date and the method of delivery, and the training content. Training records must be maintained according to applicable record keeping rules.

The policies and procedure shall be amended on a need basis. Any amendment, partly or wholly, shall remain the integral part of this policy.

**19. Investigation**

Important to remember that every explanation offered by the customer cannot be accepted without scrutiny.

**20. Threshold Transactions**

Threshold transactions, as defined by the regulatory body, refer to transactions with an amount equal to or above ten lakhs in a single day by a single person. Such transactions must be reported to the Financial Information Unit (FIU) within 15 days from the date of the transaction via the goAML application. The company shall report TTR:

- One or more transactions received by a single customer, where the amount is equal to or exceeds 10 lakhs in a single day.

*Note: Threshold transactions shall change based on changes in FIU requirements from time to time.*

**21. Suspicious Transactions**

This section is intended mainly to highlight situations that may suggest that money laundering or terrorist financing is taking place. Sometimes, individual situation/transaction may not suggest the money laundering activity but a combination and series of such situations may be indicative of such illicit transaction.

The beneficiary shall clarify the economic background and purpose of any transaction of which the form or amount appear unusual in relation to the customer.

If the suspicious transaction is identified, shall report STR to Financial Information Unit (FIU) via goAML application.

**22. Record Keeping and record retention**

Records substantiating the proper identification of customers and documenting their transactions must be made in order to provide both an audit trail and adequate evidence for the appropriate authorities. Appropriate steps should be taken to evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities. Further, the company should maintain for at least five years from the date of cessation of transaction between the company and the client, all necessary records of transactions which will permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity.

Concerned official should ensure that records pertaining to the identification of the customer and his address (e.g. copies of documents like passports, identity cards, driving licenses, PAN Cards etc.) obtained while transaction payment, are properly preserved for at least five years after the business took place. The identification records and transaction data should be made available to the competent authorities upon request.

**23. Failure to report**

CGFL's customer Service Centers, sub representative office that fails to report unusual and suspicious transactions, shall be penalized in accordance with the guidelines of Nepal Rastra Bank.

**24. Confidentiality**

No investigation officer or staff or person involved in the investigation and inquiry shall violate confidentiality of any matter or submitted documents that came to his information in the course of investigation and inquiry or in performing his duty, unless the prevailing laws requires so.

**25. Code of Conduct of employees**

- Employees must remain vigilant to the possibility of money laundering through use of CGFL's service.

- Employees must comply fully with all anti-money laundering policies and procedures in respect of customer identification, transaction monitoring, record keeping and reporting.
- Any information provided to compliance department or any information disseminate to any staff or representative while working in a normal course of work or at any time of providing to investigating unit shall not be disclosed to anybody except mandatory to disclose as per the current Act/Law.
- Employees must not inform/warn the customers about the suspicion.
- Employees must not talk/disclose with other employees and friend/family.
- Employees must comply with the instructions of the competent authority and department head that he/she has been reported.
- Employees must cooperate with the competent authorities in investigation.
- The relationship with the customer shall not be damaged if the authorities regard the remittance transaction as bona fide.
- If the customer/transaction found to be act of money laundering, the authority will be in a better position to catch the culprit and there will be less chance of eroding the evidence.
- Employees failing to report suspicious and unusual transaction shall attract legal and disciplinary action.

**26. Non Compliance with CGFL's AML/KYC Policy and procedures**

Failure to abide by the Policy and Procedures set by CGFL to prevent money laundering and terrorist financing will be treated as a disciplinary issue. Any deliberate breach will be viewed as gross misconduct. This could lead to termination of employment and could also result in criminal prosecution and imprisonment for the member of staff concerned.

**27. Undertaking under each Sub Representative Agreement**

CGFL requires obtaining 'Undertaking' for each Sub Representative Agreement, in the format as specified in **Annex 7**.

**28. Politically Exposed Persons (PEPs)**

Present potentially higher risk situations. Additional/Enhanced due diligence is required when dealing with these people. Politically exposed persons are understood to be persons entrusted with prominent public functions, their immediate family members or persons known to be close associates of such persons. Public functions exercised at levels lower than national level should normally not be considered prominent however where their political exposure is comparable to that of a similar position at the national level, they should be considered on a risk sensitive basis whether they should also be considered a PEP. The actual definition of a PEP found in the Anti-Money Laundering Directive is as follows:

a) Heads of state, heads of government, ministers and deputy ministers
b) Members of parliament

c) Members of supreme courts, of constitutional or other high level judicial bodies
d) Members of courts of auditors or of the boards of central banks
e) Ambassadors, charges d' affaires and high-ranking officers in the armed forces
f) Members of the administrative, management or supervisory bodies of state-owned companies and in each instance include the following:
g) The spouse or any partner equivalent to a spouse
h) The children and the children's spouses
i) Parents
j) Any close associate who is defined as any person who is known to have a joint beneficial ownership in a legal entity with a person listed above or has sole beneficial ownership in a legal entity that is known to have been established for the benefit of a person listed above.

*Note: Western Union always performs a PEPs screening process while sending remittances to Nepal using the Accuity compliance software.*

# Section B

**Frauds and its preventions**

1. **Fraud against the consumer**

Consumer fraud occurs when criminals convince or trick consumers to transfer money to the criminal or the criminal's associates. Criminals use a variety of scams to perpetrate such crimes, and they often target the most vulnerable members of society-particularly the elderly. It is therefore imperative that Agents are always aware of potential fraud-related activity. Consumer fraud generally involves criminals conducting scams to persuade consumers to transfer money to them that might sound financially appealing to the consumer, but are in fact an attempt to steal from the consumer.

**1.1 Common consumer fraud types**

All Associates shall be trained to recognize the following common types of consumer fraud scams so they can help protect consumers from becoming victims.

**I. Advanced Fee or Prepayment Scam**

Victim is asked to pay upfront fees for financial services which are never provided. Victims often send a succession of transactions for payment of various upfront fees. Methods: credit card, grant, loan, inheritance, investment.

**II. Charity Scam**

The victim is often contacted by e-mail, mail or phone by someone asking for a donation to be sent by money transfer to an individual to help victims of a recent current event, such as a disaster or emergency (such as a flood, cyclone, or earthquake). Legitimate charity organizations will never ask for donations
to be sent from one individual to another individual through a money transfer service.

**III. Emergency Scam**

Victim is led to believe that they are sending funds to assist a friend or loved one in urgent need. Victim sends the money with urgency as the victim’s natural concern for a loved one is exploited.

**IV. Grandparent Scam**

This scam is a variation on the Emergency Scam. The victim is contacted by an individual pretending to be a grandchild in distress, or a person of authority such as a medical professional, law enforcement officer, or attorney. The fraudster describes an urgent situation or emergency (bail, medical expenses, emergency travel funds) involving the grandchild that needs a money transfer to be sent immediately. No emergency has occurred, and the victim who sent money to help their grandchild has lost their money.

**V. Immigration Scam**

Victim receives a call from someone claiming to be an immigration official saying there is a problem with the victim's immigration record. Personal information and sensitive details related to the victim's immigration status may be provided to make the story seem more legitimate. Immediate payment is demanded to fix any issues with the victim's record and deportation or imprisonment may be threatened if payment is not made immediately by money transfer.

**VI. Employment Scam**

Victim responds to a job posting and is hired for the fictitious job and sent a fake check for job related expenses. Check amount exceeds the victim's expenses and victim sends remaining funds back using a money transfer. The check bounces and the victim is responsible for the full amount.

**VII. Lottery or other Prize Scam**

Victim is told that they have won a lottery, prize or sweepstakes and that money must be sent to cover the taxes or fees on the winnings. The victim may receive a check for part of the winnings and once the check is deposited and money is sent, the check bounces.

**VIII. Relationship Scam**

Victim is led to believe that they have a personal relationship with someone they met online often by social media, in an online forum or on a dating website. The victim is often emotionally invested, often referring to the recipient as a fiancee and believes they are sending money for travel or medical expenses. In the end, the fraudster is stealing from the victim and no relationship is every formed.

**1.2 Consumer Behavior Fraud Indicators**

- ✓ Exhibiting suspicious behavior such as loitering, failing to make eye contact, etc.
- ✓ Multiple individuals entering a location but only one transacting
- ✓ Appear confused / are unfamiliar when dealing with how to use Western Union
- ✓ Are following directions of someone on the phone or standing outside the location with regards to the money transfer
- ✓ Admit they have never met the sender
- ✓ Appear to be coached to state they have met the sender

**1.3 Consumer Transaction Fraud Indicators (Red Flags):**

- ✓ Consumers receiving transactions under different names / spelling variations
- ✓ Same / similar ID numbers/ date of birth/ address are used for multiple receivers
- ✓ Increase in receivers with IDs unusual for the location
- ✓ Consumers receiving unusual transactions amounts in a short period of time
- ✓ Single or multiple consumers receiving multiple transactions from a single sender

- ✓ Consumers receiving multiple transactions from multiple senders with no apparent family relationship
- ✓ Consumers receiving multiple transactions from multiple countries
- ✓ ID location for multiple receivers do not correlate with the transaction origin
- ✓ Receiver`s occupation does not support the number of transactions being received or the countries it is originating from.
- ✓ Consumer picking cash and handing over the cash to another person inside / outside the agent location
- ✓ Consumers collecting transaction late in the night

**1.4 KYC Questionnaire to encounter Consumer Fraud**

Open ended KYC questions with the purpose of making the receiver think about their responses. Pay attention to not only the receiver's answers to the questions, but also the receiver's behavior (do they become nervous or struggle to answer? Some of the open-ended questions are:

- ✓ "What is your relationship to the sender?"
- ✓ "Where and when did you first meet the sender?"
- ✓ "What is the purpose of the transaction?"
- ✓ "How often do you use Western Union?"
- ✓ "Were you directed to receive this transaction by someone else'?"

If the Sub-Agent determines that a fraud-induced transaction has occurred at the location, or if a consumer submits a complaint to the Sub-Agent stating that they were defrauded, they should report to the HO of CGFL.

**1.5 Proper payout procedures to prevent potentially fraud-induced transaction**

Always follow proper payout procedures, confirming that the information provided by the consumer matches what is recorded in the system: MTCN, amount, expected payout area location, originating country and sender’s name. The consumer’s receiver identification must also match what is in the system and must be current (i.e., not expired), government issued, show no signs of being altered and contain the consumer’s first name, last name and a photograph of the consumer. Scrutiny should always be given to the receiver’s identification to verify its authenticity.

2. **Fraud against the Agent**

Fraud perpetrated against the Agent location that results in a financial loss for the location Fraud against agents can happen in different ways. Below are common methods for defrauding Agents. Please note that these scenarios may not apply to all money transfer systems, such as money transfer by phone.

**I. Agent fraud perpetrated over the telephone**

Fraudsters will call the Agent location and try to induce an Associate to provide access to the Agent's computer systems. Once they have access, fraudsters use the point-of-sale system to send money without the Agent location being able to collect funds for the transaction. They can also download or have the Associate unknowingly download harmful computer viruses. The Associate must be aware of the fraud types below to help the Agent to avoid being defrauded.

**II. Remote access**

A fraudster calls an Agent location posing as Western Union or network technical services claiming that the Western Union system needs to be updated/upgraded. The Agent employee agrees to establish a personal computer support connection using remote access software. The Fraudster may then take control of the personal computer and send transactions without funds being collected by the Agent location.

**III. Computer intrusions**

An Agent employee clicks a link in an e-mail or visits a website and unknowingly downloads malicious software onto the computer offering Western Union services. This malicious software, through key loggers, captures Western Union Operator identification documents and passwords, which may be used later by fraudsters to send transactions.

**IV. Test transactions**

A fraudster calls an Agent location to have the Agent Associate enter transaction data as a test or training session which ultimately results in a transaction being sent without funds being collected.

**V. Code entries**

A fraudster calls an Agent location and instructs the Agent Associate to enter codes into the Western Union system to fix a technical issue or update the point-of-sale system. When the Agent Associate follows the fraudster's instructions, by entering a 16-digit card number and 5-digit dollar amount, the effect is to re-load a prepaid card that belongs to the fraudster.

**VI. Agent fraud perpetrated by e-mail**

E-mail fraud (also called Phishing) is designed to get the Associate or any other Agent employee to unknowingly provide the fraudster access to the Agent's internal computer systems. Phishing can also be done over a mobile phone or text. This fraud scheme is designed to steal personal information or to push malicious code or software onto the Agent's computer or mobile phone. All Associates who have access to the Agent's computers must be trained on how to avoid being the victim of phishing.

Below are indicators that the Associate can look for to help identify a potential phishing e-mail:

- an unknown sender

- an unsolicited correspondence
- an unexpected correspondence
- generic greetings
- requests for personal information
- a sense of urgency, and
- poor grammar or spelling

**2.1 Protecting The Agent from Fraud**

**NEVER:**

✓ Click on e-mails / links that look suspicious
✓ Provide your log in credentials / other sensitive personal information to anyone
✓ Enter any information into Western Union System based on a request from an incoming phone call
✓ Agree to Computer support unless you have previously initiated contact with WU or your Corporate office even if the caller says they are calling from WU or your Office`s IT team
✓ Download software from an unknown source
✓ Insert CD/USB into the PC providing WU services
✓ Enter test / training transaction in the live system

**2.2 Everyday Fraud Prevention Practices**

✓ Reviewing Fraud Awareness material provided
✓ Reviewing any Fraud alerts received
✓ Never allow consumers to see the PC screen when entering transaction information
✓ Never allow unauthorized persons behind the counter or near the WU system
✓ Never respond to e-mails, phones, etc. requesting WU information such as account numbers, terminal IDs, Operator Ids, etc.

3. **Proper payout procedures to prevent potentially fraud-induced transaction**

Always should follow proper payout procedures, confirming that the information provided by the consumer matches what is recorded in the system: MTCN, amount, expected payout area location, originating country and sender's name. The consumer's receiver identification must also match what is in the system and must be current (i.e., not expired), government issued, show no signs of being altered and contain the consumer's first name, last name and a photograph of the consumer. Scrutiny should always be given to the receiver's original identification documents to verify its authenticity.

# Section C

**Accountabilities & Responsibilities**

1. **The Board is Responsible for:**
   - Ensuring that adequate systems and controls are in place to deter and recognize criminal activity, money laundering and terrorist financing.
   - Seeking annual AML Compliance reports from the management and taking necessary decisions required to protect the CGFL from use by criminals for money laundering and terrorism financing.

2. **Management is Responsible for:**
   - Day-to-day compliance with Anti Money Laundering and terrorist financing obligations within the areas of the CGFL.
   - Ensuring that chief Compliance officer is promptly advised where there are reasonable grounds to know or suspect that transactions or instructions are linked to Criminal conduct, Money laundering or Terrorist financing.
   - Ensuring that Chief Compliance Officer is provided with all relevant information to enable a complete assessment of underlying transaction for suspicion.

3. **Operations in Charge/ Branch Manager /Sub Representative is responsible for:**
   - Effective policies and procedures are in place to guard against the CGFL becoming involved in Money Laundering activities
   - A staff is designated for ensuring that anti-money laundering policy implemented in every aspect.
   - Suspicion reports are made and acted upon promptly.
   - Policies and Procedures are being implemented effectively as communicated from time to time by the Corporate Office.
   - Reporting is in order as required by "Asset (Money) Laundering Prevention Act, 2008" and Guidance issued by Financial Information Unit time to time.

4. **Regional Representatives are responsible for:**
   - To work as a focal point and liaison with Financial Information Unit through Corporate Office, for effective implementation of this policy.
   - To provide required information to the Compliance Officer at Corporate Office of CGFL, who shall be responsible for vigilant for the suspected transaction.
   - Location Audit Tasks are to be carried out within specified area as an ongoing process and report it to Corporate office, in the format as specified as ***Annex 4***.

5. **Compliance Officer at Corporate level is responsible for:**
   - Effective implementation of Rules, Direction, Order, Circular under 'Asset (Money) Laundering Prevention Act, 2008' and other related Act of the Country by own self and through other designated staff.
   - To carry out proper identification of Customer by own self and through other designated staff.
   - Update the documentation collected in process for identification of the customers.
   - To provide information to the concerned authority as per the existing Act and/or Law.
   - Keeping abreast of all technical and regulatory developments on money laundering and advising Concerned Staff of any changes needed in policies or procedures.
   - Updating policy and procedures to reflect changes in statutory and regulatory obligations of the Financial Information Unit and any Act prevailing in the Country or circulations and operational advice,
   - Ensuring that all staffs are aware of their responsibilities and obligations, that they are adequately trained in all relevant aspects of Anti-Money Laundering procedures that records of training are kept, and that staff confirm annually that they have read and understood the policies and procedures set out in the Handbook.
   - Ensuring that policies and procedures are operating effectively and reporting on their effectiveness as per the time frame given to concerned staff. Reviewing all suspicious & Threshold transaction reports and reporting the same to Nepal Rastra Bank, Financial Information Unit and/or authority for controlling deflection of currency, in the GOAML website as specified in ***Annex 2.***
   - Representing the Company on Money Laundering matters to all relevant external agencies in the Country and aboard, ensuring that all reasonable requests for information are complied with promptly, subject to the Company's legal responsibilities on customer confidentiality.
   - The Compliance Officer will prepare a report on required basis and submit the report on CDD and Money Laundering issue. A Separate report shall be submitted for the Money Laundering issue surfaced by the Compliance Officer on case to case basis.
   - Any action taken to any Sub Representative or Termination of any Sub Agent, due to AML Compliance related matters, must be reported to NRB / FIU in the prescribed format as per ***Annex 6.***
   - The Compliance Officer will submit report to authority as required by "Asset (Money) Laundering Prevention Act, 2008" and Guidance issued by Financial Information Unit time to time.
   - Ensure that a clear undertaking has been obtained for each Sub Representative Agreement in the format as specified as **Annex 7**.

6. **All CGFL Staff and sub-representatives are Responsible for:**
   - Reading and ensuring that they understand the policies and procedures, signing to acknowledge that they have done so and providing an annual re-confirmation or within the time frame given to this effect.
   - Complying fully with all anti-money laundering procedures including in respect of customer identification, Transaction monitoring, record keeping and suspicion reporting.
   - Being alert at all times to the possibility of money laundering and reporting all suspicious or unusual transactions to the Compliance Officer.
   - Making effective use of training given seeking additional training where necessary and confirming receipt when training is given.
   - Being aware that violation of money laundering legislation could involve personal penalties including fines or imprisonment, or both; and being aware that breaches of procedures set out in this policy may be constituent Gross Negligence and may attracts disciplinary action as per the Employees By-laws.

# Annexes

**Annex -1: Procedure Regarding (Know Your Customer)**

Remittance Companies has to obtain following documents from the customers depending on the type of the customer. Further, where necessary, private interview of the customer shall also be taken.

**I. Individual Beneficiary**

1. Name & Title: As per citizenship Certificate/Driving license/ID card of Voting right or Passport.
2. Permanent Address (Documents evidencing the address): as per citizenship
3. Temporary Address (Documents evidencing the address)
4. Telephone/Mobile Number
5. Copy of Citizenship Certificate/Driving License/ Passport/Voters ID/PAN Card (Number and description)
6. Copy of Identity Card in case of employees working in partly or fully Government owned corporations.
7. Sources of Fund
8. Relationship to Sender
9. Occupation
10. Clear Signature
11. In case of foreign Nationals: Passports with valid visa or in exception case Certificate issued by foreign Embassy held at Nepal
12. In case of Indian Nationals: Copy of Passports or Certificates issued by Indian Embassy held in Nepal (Photo must be attached in such certificates).
13. Tibetan/Bhutanese/Other Refugee- Refugee ID issued by Ministry of Home- Nepal Govt/IOM.

**II. Sub Agency Agreements with Partnership Firm**

1. Firm's Name: As per registration Documents.
2. Address of the firm: As per registration Documents.
3. Telephone Number
4. Name and Address of the partners: As per partnership deed.
5. Firm Registration Certificate and PAN certificate
6. Partnership Deed.
7. Copy of Citizenship Certificate or any valid government issued ID card of the Partners
8. Authorization documents for financial and administrative task
9. On Top of all, a Letter of Interest (LoI) has to be submitted to CGFL. The LoI should be in the format as specified in Annex 3.

**III. Sub Agency Agreements with Proprietorship Firm**

1. Name of the Firm: As per registration documents
1. Address: As per registration documents
2. Name and address of proprietor
3. Firm Registration Certificates and Pan Card
4. Copy of Citizenship Certificate of the proprietor or any valid government issued ID card
5. On Top of all, a Letter of Interest (LoI) has to be submitted to CGFL. The LoI should be in the format as specified in Annex 3

**IV. Sub Agency Agreements with Companies**

1. Name of Company: As per registration documents.
2. Address of Corporate and concern Branch office:
3. Telephone/Fax Number
4. Certificate of Incorporation, Memorandum and Article of Association
5. Income Tax registration (PAN) and Clearance (If any) Certificate
6. Name and Address of the Board members (BOD)
7. Board resolutions for carrying out the business with an authority to Managing Director and other authorized officials
8. Citizenship/identification and photos of sub representative's business representative
9. On Top of all, a Letter of Interest (LoI) has to be submitted to CGFL. The LoI should be in the format as specified in **Annex 3**

**V. Sub Agency Agreements with Companies Co-operative societies, Clubs, Societies, Association, Trusts**

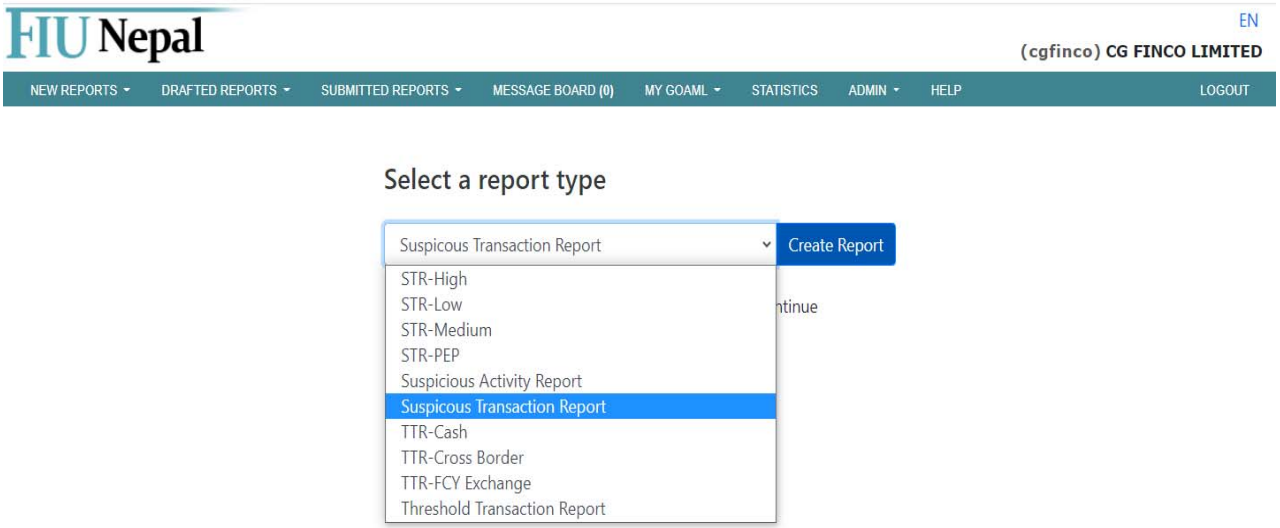
1. Name and address of the organization: As per registration documents.
2. Registration certificate
3. Constitution and by laws
4. Name and address of executive committee/council
5. Telephone number
6. Resolution of the Board/Executive committee for sub representative
7. Authorization from the board or Executive committee for remittance business and signatories to the business.
8. Tax exemption certificate from Internal Revenue Department (If applicable as "Nil" rate of TDS)
9. On Top of all, a Letter of Interest (LoI) has to be submitted to CGFL. The LoI should be in the format as specified in Annex 3

**VI. Sub Agency Agreements with Public/Private Trust**

1. Name of Trust
2. Address

3. Constitution of Trust
4. Trust Deed
5. Name and address of trustees
6. Registration Certificate
7. Name and address of Managing committee.
8. Telephone number
9. Board/Managing committee's decision for sub-representative's business.
10. Other relevant documents.
11. On Top of all, a Letter of Interest (LoI) has to be submitted to CGFL. The LoI should be in the format as specified in Annex 3

**Annex 2: FIU-Nepal, GOAML Website for reporting Threshold and Suspicious Transactions:**

## Annex 3: Format for 'Letter of Interest (LoI)' from interested party/ies to work as a sub-representative

*Annexure 1 (SOP v2.0 Nepal)*

**APPLICATION FORM FOR SUB-AGENT OF WESTERN UNION**
**(वेष्टर्न यूनियनको सब-एजेन्ट आवेदन फाराम)**

Date (मिति): _____/____/____

I/we hereby express our interest to become a Sub-Agent of Western Union Money Transfer and apply for the same including herewith all required documents to the main agent mentioned below (म/हामी वेष्टर्न यूनियनको सब-एजेन्ट हुन ईच्छा गरी सो पाउनकालागि तल उल्लेखित वेष्टर्न यूनियनको मुख्य एजेन्ट मार्फत् सँस्थाको आवश्यक सम्पूर्ण कागजातहरु यसै आवेदन फारमसाथ सँलग्न गरी पेश गरेको छु/छौं ।)

**Application submitted to Main Agent (कागजात पेश गरेको मुख्य एजेन्ट):**

Agent Name(एजेन्टको नाम):

Agent Address(एजेन्टको ठेगाना):

**Details of Applicant Firm/Company (निवेदक सँस्था/कम्पनीको विवरण):**

- Name (नाम):
- Municipality/GP (न.पा./गा.पा.): Ward No. (वार्ड नं.):
- City (शहर/ठाँउ): District (जिल्ला): Province (प्रदेश):
- Phone No.(फोन नं.): Reg No. (दर्ता नं.):
- PAN Number (प्यान नं.):
- Authorized E-mail Address (आधिकारिक इमेल):
- Name of Proprietor/Director (प्रोपाइटर/सञ्चालकको नाम):

I/we also declare that (म/हामी यो पनि उद्घोष गर्दछु/गर्दछौं):

1. I/we have not filled-up the form for a sub-agent of Western Union Money Transfer and also have not forwarded documents of our firm/company to any main agent of Western Union prior to this application. (म/हामीले यस निवेदन भन्दा पहिले वेस्टर्न यूनियनको सब-एजेन्ट बन्नकालागि कुनैपनि आवेदन फारम भरेको छैन । र, यस सँस्थाको कागजातहरु समेत वेष्टर्न यूनियनको कुनैपनि मुख्य एजेन्टलाई उपलब्ध गराएको छैन ।)
2. If a breach of point (1) is proven in future, we agree to accept any action taken as per Western Union policy. (भविष्यमा यदि माथिको बुँदा (१) उलङ्घन भएको पुष्टि भएमा म/हामी वेस्टर्न यूनियनको नीति अनुसार हुने कुनै पनि कारवाही स्वीकार गर्न सहमत छु/छौं ।)

The information mentioned above are true and correct (माथि उल्लेखित सबै सूचनाहरु सही र सत्य छन् ।)

Authorized Signature (आधिकारिक दस्तखत): _____

Name of authorized person (आधिकारिक व्यक्तिको नाम): _____

Designation (पद): _____ Mob. #(मोबाइल नम्बर): _____

_____
Office Stamp(mandatory) कार्यालयको छाप (अनिवार्य)

**Annex 4: Format for 'Location Audit" (Checklist). Location audit to be carried out by Regional Representatives as an ongoing process**

CG फिन्को
विश्वसनीयताको अनुभूति

WESTERN UNION
moving money for better

**Annex-4**

## Individual Sub-Agent Review Form

**Sub-Agent Name:** ..... **Date:** .....

**Address:** .....

**Account Number:** .....

| | | | | | |
|---|---|---|---|---|---|
| 1 | Received adequate training of WU Payment Process | | Yes | | No |
| 2 | Authentic IDs copy after verification with original one are obtained for every transaction | | Yes | | No |
| 3 | Proof of Payment (POP) related documents are safely stored at least for 5 years | | Yes | | No |
| 4 | Adequate knowledge about NRB's rules, WU guideline & regulations about remittance an its Implementation | | Yes | | No |
| 5 | Suspicious and/or Threshold Transaction been paid by the Location | | Yes | | No |
| 6 | Sub agents are making payment to the customer via cheque/bank transfer exceeding the transaction fixed by NRB | | Yes | | No |
| 7 | Read and understood the provisions of CG Finco's KYC & AML/CFT Compliance policy manual | | Yes | | No |
| 8 | Adequate knowledge about obtaining disclosure from the beneficiary upon Relationship between Sender & Receiver and Purpose of Remittance | | Yes | | No |
| 9 | Instant payment of full amount under each transaction paid by Location | | Yes | | No |
| 10 | Fraud Related Training (Consumer Fraud & Agent Fraud) | | Yes | | No |

Above checklist are specifically designed to carry-out Inspection /Audit by any CG Finco or Western Union officials as an ongoing process, and with or without any prior information. Any violation or misconduct to this checklist may attract a serious action by CG Finco &/or Western Union.

All above information is true and correct. I/We have read & understood the terms & Conditions prior to sign it.

**Reviewer**

**Name:** .....

**Signature:** .....

**Sub-Agent**

**Name:** .....

**Operator ID:** .....

**Signature:** .....

**Company Seal:** .....

CG Finco Sub-Agent Review Form 2022

**Annex 5: Format for 'Training/Instructions" to the Sub-agents.**

CG फिन्को
विश्वसनीयताको अनुभूति

WESTERN UNION
moving money for better

Annex-6

## Sub-Agent Training Form

**Sub-Agent Name:** ..... **Date:** .....

**Address:** .....

**Account No.:** .....

**Topics for Training Program:**

| | | | |
|---|---|---|---|
| 1 | **Payout Transaction – Basic Requirements** | | |
| | • MTCN | • Sender/receiver Name | • Origin of Funds |
| | • Funds | • Identification | • Statutory Disclosure (Purpose of transaction, Relationship to the Sender) |
| 2 | **Identification** | | |
| | • Citizenship Card | | • Passport |
| | • Driving License | | • PAN Card for Individuals |
| | • Election Voter Card ID | | • Refugee Card |
| | • Government Staff ID (generally of Police, Army, Bureaucrats) | | |
| 3 | **Customer Due Diligence** | | |
| | Due diligence required for the transaction that have unrelated sender and receiver originating from high risk countries. Due diligence includes-Purpose of transaction, Relationship, Does receiver has met the sender? | | |
| 4 | **Compliance** | | |
| | • AML/CFT policy | • Data Integrity | • Suspicious/Fraud Transactions |
| 5 | **The Rules of Doing Business** | | |
| | • Remittance Payment | | • Remittance Purpose |
| | • Payment Restrictions | | • Remittance Ceiling |
| | • Hoarding of Customers | | • Confidentiality |
| 6 | **The DONTS** | | |
| | • Location Shifting | | • Unauthorized Transaction Processing |
| | • Location Poaching | | • Poor Visibility |
| 7 | **Proof of Payment** | | |
| | • Automated Customer Receipt (ACR)-Final Print | • Self Attested ID Card | |
| 8 | **Nepal Rastra Bank Guidelines** | | |
| | • Know your customer | • Monitoring & reporting of Threshold & suspicious Transaction | • Record keeping & record retention |
| 9 | **Fraud activity and its prevention** | | |
| | • Know Your Employee | • Fraud against consumers and Agents | • Prevention & Control |

**Trainer**

**Name:** .....

**Signature:** .....

**Trainee**

**Name:** .....

**Operator ID:** .....

**Signature:** .....

**Seal:** .....

CG Finco Sub-Agent Training Form 2022

**Annex 6: Format for 'Action taken / Termination of Sub-representative' reporting to Nepal Rastra Bank**

# CG Finco Ltd.

## Sanepa - 2, Lalitpur

**List of Sub agents / Sub Representative Terminated/Action taken for the Month of .....**

| S.No. | Name of Sub Agent / Sub Representative | Address | Date of Appointment | Date of Termination / Action Taken | Due Payment to the Customer | Due Payment to the Sub Agent | Reason for Action taken / Termination |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

## Annex 7: Format for 'Undertaking by Sub Representative'

Date:

To,
CG Finco Ltd.
Sanepa – 2, Lalitpur
Nepal.

**Subject: Undertaking**

I/We have received, Read and understood the KYC AML/Compliance Policy of CG Finco Ltd. and I/We hereby undertake to comply, observe and be bound by the Terms and Conditions made here under this Policy and as may be amended by CGFL from time to time. We also undertake to indemnify CGFL against any loss, damages, costs (including any legal costs) or demands as incurred by CGFL as a result of or in connection therewith.

Name of Sub Representative :

Address :

Phone No. : Mobile No.:

Signature of Authorized person :

Name :

Designation : Company Seal: