AML / CFT AND SANCTIONS POLICY

CONTENTS

1. Document Overview

1.1. Purpose

Criminals accumulate significant sums of money by committing crimes such as drug trafficking, human trafficking, theft, card fraud, extortion, corruption, embezzlement etc. Money laundering is a serious threat to the legal economy and affects the integrity of institutions. It also changes the economic power in certain sectors. If left unchecked, it will corrupt society as a whole.

CAPOLIN, S.R.O. (hereafter CAPOLIN that operates under ZOAN trademark) does not tolerate any illegal or illicit activity from either its customers, partners or its own employees, and CAPOLIN is committed to the highest standards for preventing money laundering, financial crime (including bribery and corruption), terrorism financing and other acts punishable by respective legal acts.

This Policy outlines the principles, objectives and requirements, including internal safeguards and customer due diligence duties, training requirements, employee responsibilities, monitoring of suspicious occurrences and transactions, that underpin CAPOLIN's commitment to combating and preventing money laundering, financial crime, terrorism financing.

The nature of the operation of CAPOLIN calls for international interaction. The legal, reputation, operation and concentration risks have prompted a number of self- regulatory actions by the industry. As a result, current Policy and related procedures are driven by standards and regulations of both the FATF and US, EU and internationally accepted best practices.

The purpose of this Policy is to provide guidance relative to managing banking regulations such that compliance for CAPOLIN Clients management and payment Programs is ensured and ML and other related risks are controlled.

Related Documents include:

- Third Party Vendor Management Policy and Procedures; and
- Fraud Management Policy and Procedures.

1.2. Objectives

Establishing a "best practice" for managing AML Compliance and implementing a standard set of Policies and Procedures will allow CAPOLIN to achieve the following objectives:

- Develop and maintain tracking and reporting of AML and regulatory oversight in order to identify and remediate non-compliance issues;
- Establish a process to ensure the AML Compliance Policy and Procedures are updated to reflect the current business environment.
- Effectively meet all the requirements of "Know your Customer" process;
- Comply with sanctions regimes and implement automated systems to check and validate any transactions that may be related directly or indirectly to a sanctioned individual or entity;
- Abide by the FATF recommendations and Wolfsberg Group Guidance, especially those related to KYC

- Establish a clearly defined process for enforcing and auditing AML Compliance Policy and Procedures. Define review periods and publication dates.
- Easily maintain version control; and
- Identify Subject Matter Experts (SMEs) with clear accountability and responsibility.
- Ensure that CAPOLIN and its staff will not knowingly assist anyone to launder the proceeds of drugs sales, illegal businesses, embezzlement, terrorism, or other acts prohibited as predicative offences.

1.3. General Policy Statement

CAPOLIN shall handle AML and other regulatory compliance in a consistent manner that minimizes the risk of compliance violations. AML Procedures shall be managed in accordance with the procedures noted below so that compliance optimizations always considered.

CAPOLIN acknowledges the global character of the risks arising from money laundering, terrorism financing, financial crime, fraud, and other acts punishable by law, and realizes that it is indispensable to implement a group-wide approach when managing risks in this area. Therefore, CAPOLIN is convinced that all participants/representatives of CAPOLIN must have systems and processes in place to monitor and share information on the identity of customers if a suspicion of criminal involvement arises, and to be alert to customers using CAPOLIN's services in ways which are incompatible with CAPOLIN's policies and procedures and business approach.

CAPOLIN shall implement and monitor policy and procedures for the governance of AML Compliance and associated risk. This process shall include the following policy and procedures:

- Overall governance–approval and control.
- Standard operating procedures for handling risk.
- Ongoing monitoring.
- Defined SME roles and responsibilities.
- Defined review frequency; and
- Staff education and training.

It is the responsibility of CAPOLIN management to ensure compliance with this Policy. The Chief Compliance Officer (CCO) will review this policy at least annually. Outside of the designated review frequency, the CCO is responsible for monitoring the AML Compliance Policy and Procedures enforcement with CAPOLIN participants (internal and external).

The CCO is responsible for ensuring that internal policy and procedures associated with the AML Compliance Policy are properly implemented and effective, including any exceptions to AML Compliance Policy granted by appropriate CAPOLIN management.

1.4. Policy Compliance

Non-compliance with this Policy may lead to disciplinary action by CAPOLIN, up to and including dismissal of any participants.

2. Introduction

2.1. Background Information

CAPOLIN is responsible for:

- Management and direct control over the Clients management, cryptocurrencies transactions, payment methods and card programs following the requirements set by the Financial Regulators.
- Contracting with service providers such as Processor that are approved by the Issuing Bank.
- Managing Card Programs and Program Partners.
- Customer Service.
- Fraud losses; and
- Managing AML/CFT and Sanctions Programs.

CAPOLIN will oversee and manage Clients, cryptocurrencies transactions, payment methods and card programs, which includes, without limitation, paymaster, reloadable, travel, and corporate gift/incentive programs.

CAPOLIN focuses on following key pillars to enable its business and services:

- Strong identity verification technologies and mechanisms.
- Robust biometric verification.
- Additional verification services on scoring, reputation, or fraud prevention.
- Business rules associated with the onboarding process (acceptance, rejection, identity verifications, AML sanctions lists, etc.).
- Efficient security checks in accordance with regulations.

2.2. Policy

This Policy embodies a risk management and compliance program undertaken by CAPOLIN to ensure that AML/CFT requirements are followed. It has been approved and adopted by the Board of Directors of CAPOLIN as of the date set forth on the cover of the Policy. At least annually, CAPOLIN will reaffirm its commitment to the principles embodied in this Policy; and no later than the ninety (90) days after closing its fiscal year, the Board of Director(s) shall evaluate the effectiveness of the Policy, make all required amendments, and re-assert in its minutes CAPOLIN's Board of Director's approval and adoption of same.

CAPOLIN's AML/CFT and Sanctions Program is comprised of (i)this Policy, (ii) CAPOLIN's internal controls, (iii)designation of a Compliance officer, (iv) appropriate record keeping and reporting, (v) required record retention, (vi) internal random testing and review of compliance procedures and knowledge, (vii) an independent audit of its compliance principles and program, (viii) the training of personnel (as appropriate),and(ix)its mechanism for updating policies and procedures.

Anti-money Laundering and Combating the Financing of Terrorism regulations and related laws require CAPOLIN to take reasonable steps to verify the identity of its customers, monitor and report certain currency, suspicious and foreign transactions, and maintain specific records. These steps require CAPOLIN to keep records that provide an audit trail that law enforcement can utilize and provides penalties for individuals and entities attempting to avoid those requirements.

The Policy is established on a risk-based approach that is at the heart of CAPOLIN's framework for anti-money laundering and counter terrorism financing as well as the prevention of financial crime and other acts punishable by law taking into consideration the geography, customer type, as well as products and services served.

This Policy complies with all regulations and requirements of CAPOLIN and the applicable regulations for the Clients management, cryptocurrencies transactions, payment methods and card programs. This Policy is intended to educate and promote secure behavior by employees and participants (Program Partners and Service Providers/Vendors) of CAPOLIN:

- Comply with CAPOLIN policies and procedures.
- Comply with applicable U.S., EU, and Generic regulatory requirements.
- Comply with FATF recommendations.
- Detect and prevent money laundering and terrorist financing.
- Identify all risks, which will allow CAPOLIN to determine and implement proportionate measures and controls to mitigate these risks.
- Recognize the penalties of noncompliance.
- Ensure compliance by any third-party providers.
- Identify suspicious activity and transactions.
- Maintain proper records and reporting.

CAPOLIN, the Board of Directors, officers, employees, and CAPOLIN agents will not be held liable to any person for reporting suspicious transactions on the Reportable Activity Referral (RAR) form. In addition, it is against the law to tell a suspect about the information reported on the RAR form, or that a RAR form has been completed.

CAPOLIN will perform new and continuing training to ensure employee compliance with all aspects of this document and underlying policies and procedures. CAPOLIN will perform oversight review of training to ensure other participants are also incompliance with this Policy.

Although this document may contain legal information, it is not intended to be, nor shall it be considered, legal advice. Refer to Appendix C for Sample RAR Form.

2.3. Policy Statement

2.3.1 General

It is the policy of CAPOLIN to comply with the letter and the intent of all provisions of AML/CFT regulatory

requirements by establishing this Policy as CAPOLIN's written Policy and Compliance Program.

2.3.2 AML/CFT Compliance Program Goals

Goals of CAPOLIN's AML/CFT Compliance Program consist of:

- A system of internal controls to ensure ongoing compliance for all operations of the prepaid Card Program.
- Established procedures to verify the identity of a person who be a Client, cryptocurrencies transactions, obtain payment methods and card programs identifying information concerning such person using automated data processing systems.
- Independent audits and testing to ensure ongoing compliance conducted by CAPOLIN personnel or a third-party entity consultant.
- Designation of an AML/CFT Compliance Officer responsible for coordinating and monitoring day-to-day compliance; and periodic training of CAPOLIN's appropriate personnel concerning their responsibilities under the program, including training in the detection of suspicious transactions and frauds.

All CAPOLIN employees are responsible for compliance with all AML/CFT requirements outlined in this Policy.

CAPOLIN has voluntarily adopted an anti-money laundering policy to adhere to the legal and regulatory schemes governing its activities. Specifically, it is CAPOLIN's policy that:

CAPOLIN will appoint a qualified employee (in a position of responsibility) as an AML/CFT Compliance Officer ("Compliance Officer") who shall have day-to-day responsibility for managing all aspects of the AML/CFT compliance program, including compliance with all AML/CFT regulations. The Compliance Officer may delegate certain AML/CFT duties to other employees, but not compliance responsibility. Pursuant to the authority contained in the Corporate Resolution approving this Compliance Program, the Compliance Officer shall have sufficient authority and resources to effectively administer a comprehensive AML/CFT compliance program. The Compliance Officer shall act in independently (to the extent possible, taking into consideration the size and capabilities of staff) of all other departments and divisions (in particular, audit, sales, and implementation departments) and shall report directly to the Chief Executive Officer of CAPOLIN. The Compliance Officer is authorized to take all steps required to ensure complete compliance with any and all applicable anti-money laundering requirements;

CAPOLIN has adopted a policy of ensuring, through due diligence, that suspicious activities are reported in the course of a transaction, if warranted. CAPOLIN also reserves the right to voluntarily file an RAR form if it becomes aware of a suspicious transaction. Additionally, certain CAPOLIN Client, cryptocurrencies transaction, payment methods or card program are or might become incapable of meeting the threshold amount requirements for the filing of an RAR form. CAPOLIN acknowledges that RAR forms should also be filed on transactions that, although they do not reach the requisite threshold amount, in instances of evidence of possible violations of the AML/CFT, or present evidence of possible money laundering. If encountered, CAPOLIN will voluntarily file a RAR.

CAPOLIN will use technology, software, trained personnel, third party entities, and all available tools to continuously monitor all transactions processed by the Client, cryptocurrencies transaction, payment methods or card program. If questions arise or should arise about the legality of the source of the funds being remitted, CAPOLIN's staff, Third Parties, where applicable, shall question customers about the source of the funds, the customer's occupation, and if appropriate, follow the procedures for filing a RAR form in conjunction with CAPOLIN's Compliance Officer; and Periodically, CAPOLIN will train all employees, managers, and directors about the anti-money laundering laws and CAPOLIN 's Compliance Program.

2.3.3 Enforcement

The primary responsibility for enforcement of this Policy and its operating procedures rests with the Compliance Officer and CAPOLIN employees.

No part of this Policy or its supporting operating procedures should be interpreted as contravening or superseding any other legal and regulatory requirements placed upon CAPOLIN. Protective measures should not impede other legally mandated processes such as records retention or subpoenas. Any conflicts should be submitted immediately to the Compliance Officer for further evaluation and/or subsequent submission to CAPOLIN's legal counsel.

CAPOLIN's Compliance Officer is responsible for:

Ensuring overall compliance with corporate policies and procedures contained in the AML/CFT Program.

Ensuring that CAPOLIN is in compliance with the obligations stipulated under anti-money laundering and counter terrorism financing legislation applicable for CAPOLIN.

Performing all tasks with regard to the prevention of money laundering, terrorism financing and other acts punishable by law within CAPOLIN companies.

Overseeing the reporting process to ensure all required reports and records are maintained in compliance with the regulatory, Client on barding, cryptocurrencies transaction, payment methods or card program and requirements.

Monitoring changes in the prepaid business, as well as laws, regulations, and industry best practices to ensure AML/CFT program remains updated as necessary and reflects current standards.

Investigating indications of money laundering by clients in the first instance.

Developing and implementing a training program to ensure all employees receive adequate training and understand the importance of compliance; and serving as the designated person to whom suspicious activity is referred. Submitting RAR forms as needed.

3. Anti-Money Laundering (AML)/Combating the Financing of Terrorism (CFT) and Sanctions Program

CAPOLIN recognizes that the potential of risks and penalties exists in the ever-changing regulatory environment, and in response has developed and implemented a comprehensive risk-based AML/CFT and Sanctions Compliance Program. This Program includes:

- A comprehensive Program Risk Assessment to identify risks associated with Card Program geographies, customers, products and services, and the nature of CAPOLIN's operations.
- Policies, Procedures and Processes.
- A system of internal controls, including a process for the identification and mitigation of gaps in those controls.
- Independent testing and auditing.
- Designated individuals responsible for monitoring day to day compliance; and
- Periodic training of all employees that ensures this and other related policies, procedures and processes are shared and communicated with all business lines across CAPOLIN, including its Board of Directors, Senior Management, and employees.

3.1. Program Risk Assessment

CAPOLIN has a Risk Assessment Program for evaluating risks based on the customer, product, third party service providers and geographic attributes of a Clients, cryptocurrencie transaction, payment method and card program. All the events are designed to meet all requirements specified, with regard to AML/CFT, OFAC/UNSCR other relevant watch list checks, transaction monitoring, and reporting. CAPOLIN has an AML/CFT program. CAPOLIN will perform new and continuing training to ensure employee compliance with all aspects of the Policy and underlying policies and procedures.

CAPOLIN also conducts contractual third party independent testing and auditing of its risk assessment process for reasonableness. Additionally, it is the responsibility of Senior Management to ensure CAPOLIN personnel are staffed and properly trained to promote adherence with this Policy and other policies, procedures and processes based upon its risk profile. A high-risk profile requires a more robust program that specifically monitors and controls the higher risks that Senior Management and the Board of Directors have accepted.

CAPOLIN's AML/CFT, AML and OFAC/UNSCR other relevant watch list SANCTIONS risk assessment program is an ongoing process. It is the responsibility of Senior Management to ensure CAPOLIN's risk assessment is updated every 12 to 18 months to identify changes in CAPOLIN's risk profile (e.g., when new products and services are introduced, changes to existing products and services, high risk customers, open and closed card accounts, CAPOLIN expands through mergers and acquisitions).

3.1.1 Specific Risk Categories

The results of money laundering and terrorism financing risk assessments serve as the starting point for the risk-oriented strategy regarding internal safeguard measures and risk-based customer due diligence procedures of CAPOLIN.

The first step of the risk assessment process is to identify the specific products, services, customers, entities, and geographic locations unique to the Program.

CAPOLIN has identified the following risk categories for the clients, cryptocurrencies transactions, payment methods or card programs:

- Product Risk.
- Geographic/Country Risk.
- Customer/Client Risk; and Third Party Risk

The risk assessment is done based on risk- scoring model of at least three-dimensional matrixes to determine the appropriate risk weights, which are constantly adjusted whenever the associated risk categories change. These risk categories are detailed as H (High),M (Medium),or L (Low) .

3.2. Risk Summary

3.2.1 Geographic /Country Risk

A crucial step in devising a risk-scoring model involves jurisdictional risk. It is important to assess the risks of countries or jurisdictions where individual customers reside and the risk of countries of individual customers' citizenship.

For legal entities and third party vendors, partners the risk of countries where the corporate customers are headquartered and where they conduct the majority of their business should be assessed.

Country risk, in conjunction with other risk factors, provides useful information as to potential money laundering and terrorism financing risks. Factors that may result in a determination that country/jurisdiction/territory poses high risk are:

- Country is subject to sanctions or prohibitions set by UNSCR.
- Country is subject to sanctions set by OFAC.
- Country is identified by FATF as a non-cooperative jurisdiction.
- Country is identified by credible sources as providing funding or support terrorist activities.
- Country is identified by credible sources as having significant levels of corruption or other criminal activity.
- Country with ties to terrorist organizations and / or the territory, which is bounded by the area controlled by the terrorists.
- Country is identified as a Conflict zone a place that is characterized by the serious instability, including military circumstances, armed conflicts, or activities of terrorist organizations.
- Country has been actively attracting funds for terrorist attacks.
- Country that serves as a transit corridor to moving foreign terrorist fighters or the cash flow.
- Countries that have many deficiencies in terms of anti-money laundering and terrorism financing issues.
- Country is widely known to have high levels of internal drug production or to be in drug transit regions.
- Country is considered as an offshore jurisdiction, offshore financial center, and tax haven.

Based on the above-mentioned CAPOLIN can assign the geographic/country risk for its business as Medium or High**.**

3.2.2 Customer/ Client Risk / Cards Programs.

Implementing a strong screening process when on boarding a customer and throughout the duration of the relationship are key components to identifying high risk customer types.

For the assessment of client risk, it should be considered the personal and business sphere analysis of the client.

Given that the CAPOLIN clients, must be primarily funded through corporate funds and the Cardholders are known to the corporate client, the "Customer Risk" in this case is categorized as **Low or Medium**., unless the customers are PEP's or PEP's associates.

ID is verified through corporations and cardholders are employees or members. CAPOLIN Program Partners are corporate entities as confirmed through KYP/PDD process as stated in the Third-party Vendor Management Policy and Procedures document.

The following limits have been put in place to identify and or prevent suspicious use of the card product (where applicable):

- CAPOLIN cards will not be issued to anyone without a verifiable government ID (where KYC is required).
- Clients will be subject to identity verification through the Processor (where KYC is required).
- OFAC/UNSCR other relevant screening will be performed on each card applicant prior to approval.
- OFAC/UNSCR other relevant watch lists screening will be re-checked every 3 months – this check will be system triggered for every card holder through the Processor.
- Applicants who fail either identity verification checks or OFAC/UNSCR checks, or CAPOLIN is unable to verify customers by using automated data processing systems, will not be issued a card; and
- Due diligence will be conducted on each business who participates in the Card Program.

When an OFAC/UNSCR or other relevant watch list hit occurs, CAPOLIN does not issue a card to the applicant. CAPOLIN reports the OFAC/UNSCR hit to the Program Partner and asks the Program Partner to provide evidence that the card applicant is not the individual on the OFAC/UNSCR lists. If the Program Partner fails to provide this evidence, the card application for that card holder is denied.

When during the automated checks it is identified that the customer is PEP or PEP associate, CAPOLIN may accept that customer only after complying with the following two (2) conditions:

- When there is proof that, the individual is an honest person that truly fulfils all his responsibilities and obligations. For verification, he must submit personal, financial, and banking references.
- When the Board of Directors has approved for that particular individual.

If CAPOLIN fails to gather relevant evidence that the individual is an honest PEP or PEP associate, the card application for that card holder should be denied.

CAPOLIN periodically reassesses its OFAC/UNSCR risks and makes adjustments to its program and/or internal controls accordingly.

3.2.3 Product/Services Risk

Determining the potential money laundering risks presented by products and services assists in overall risk assessment. The Card Program are corporate-loaded and, therefore, have a **Low** risk.

3.2.4 Third Party Risk

CAPOLIN has made every effort to establish rigorous internal controls, processes, policies, and procedures to maintain compliance in all areas. Therefore, "Third Party Risk" has been evaluated as **Low or Medium.**

CAPOLIN will also conduct contractual third party independent testing and review of its risk assessment process for reasonableness. Additionally, it is the responsibility of Senior Management to ensure personnel are staffed and properly trained to promote adherence with Third Party Risk and other policies, procedures and processes based upon its risk profile. A high-risk profile would require a more robust due diligence process that specifically monitors and controls the higher risks that Senior Management and the Board of Directors have accepted.

3.3. Internal Controls

CAPOLIN's AML/CFT Program includes ensuring that they provide adequate internal controls specific to:

- Identifying the person responsible for AML/CFT and OFAC/UNSCR compliance.
- Providing adequate employee training and supervision
- Periodic independent testing.
- Identifying and reporting unusual or suspicious activity.
- Responding to government and law enforcement requests.
- Collecting and verifying customer identity, and retaining access to the information.
- Monitoring and reporting cash transactions that meet reportable threes holds.
- Creating and retaining records, such as training logs, suspicious activity reporting, currency transaction reporting and supporting documentation.
- Screening for OFAC/UNSCR violations, including initial and ongoing checks, reporting of hits, and process to block activity in OFAC/UN SCR-sanctioned countries.
- Applying third party management processes.
- Written policies and procedures reasonably designed to ensure compliance with the AML/CFT and OFAC/UNSCR.

- Training program (varying levels) for employees and/or all responsible parties including Board of Directors; and independent review of the AML/CFT Program.

Internal controls include the policies, procedures, and processes CAPOLIN has developed to provide for compliance with applicable laws and regulations. CAPOLIN has made every effort to exhibit an exceptional presence of internal controls, processes, policies, and procedures to maintain compliance in all areas.

In particular, the key controls are:

- Know Your Customer/Customer Due Diligence (KYC/CDD);
- Know Your Partner/Partner Due Diligence (KYP/PDD);
- Know Your Employer/Employee Due Diligence (KYE/EDD);
- Transaction Monitoring and Referrals of Suspicious Activity; and
- Sanctions and Restricted Countries Management.

These controls are outlined in detail in this Policy as well as in the Third-party Vendor Management Policy and Procedures and the Fraud Management Policy and Procedures.

3.4. Know Your Customer/Customer Due Diligence (KYC/CDD)

CAPOLIN has implemented a "Know Your Customer/Customer Due Diligence Policy" to meet regulatory requirements for the identification and verification of any new customer opening an clients account, cryptocurrencies transactions, payment methods and card program.

CAPOLIN has improved its ability to identify customers and verify their identity related information monitor transactions by applying new technologies that rely on advanced analytical techniques, including artificial intelligence and machine learning. Identification of customers includes comparing customer and partner's data against various external data sources, which are used to understand and verify the authenticity information and data provided by customers and partners.

The digital onboarding process helps CAPOLIN to increase its systems security and reduce fraud as it uses numerous tools for checking the customers identity. Digital onboarding process, makes it possible to use reliable technology tools to run liveness checks, face and photo liveness verification and guided interviews, when needed.

3.4.1. Customer Notification

CAPOLIN requires that within the KYC/CDD, all customers, individually or through corporate clients, be given adequate notice that information will be requested to verify their identity. The notice is provided in a manner that reasonably allows a customer to view or receive the notice before the clients account, cryptocurrencies transactions, payment methods and card program is opened. Examples include posting the notice on the application page(s) of a web site, posting a sign, printing on an application or other marketing material, or orally providing the notice. Sample language that describe the identification requirements, is as follows:

IMPORTANT INFORMATION ABOUT PROCEDURES FOR OPENING A NEW ACCOUNT—

To Help the government fight the funding of terrorism and money laundering activities, federal law requires all financial institutions and their third parties to obtain, verify, and record information that identifies each person who opens an account. What this means for you: When you open an account, we will ask for your name, address, date of birth, and other information that will allow us to identify you. We may also ask to see your drivers license or other identifying documents.

3.4.2. Collection of Customer Information

Customers will provide the following information prior to activation of the account (where KYC is required):

- Legal Name.
- Permanent Residential Address. This must be a physical address. Post Office Boxes are not acceptable, but Army or Fleet Post Boxes (APO/FPO) are allowed.
- Date of Birth.
- Identification which contains a unique identification number and a photograph and signature.
- Country of Birth.
- Nationality.
- Telephone Number or email address (both preferred).
- Signature, or electronic signature, for cards obtained on-line.
- Source of funds.
- PEP indicia.

3.4.3. Verification of Customer Information

CAPOLIN requires verification of enough customer information to reasonably validate customer identity. Depending on the process, the verification may be done face-to-face or non-face-to-face. CAPOLIN does not open accounts for which identity cannot be reasonably verified. In addition, if the circumstances surrounding the lack of verification are suspicious, CAPOLIN will report this suspicious activity on a Reportable Activity

Referral (RAR) form.

Face-to-Face Customers

Customer identity should be verified by comparing valid government-issued identification containing a photograph, against the person applying for the account and the information provided.

The following forms of valid and unexpired IDs, all of which must contain a photograph and signature will be accepted:

- Passport.
- Military ID Card.
- Driver's License or equivalent; or
- Other government-issued documentation that established the identity of the individual.
- At least two data points will be confirmed when conducting customer due diligence in person:
- Verify signatures, as well as photo to person.
- Verify the permanent address supplied to name by reviewing the photo ID provided; if ID does not match, one of the following will be used to confirm address to name:
- Utility bill.
- Tax assessment.
- Bank or credit card statement.
- Letter from public authority.
- Verify date of birth supplied to name by comparing to date of birth listed on photo ID provided; or
- Verify ID number supplied to name by reviewing the ID number listed on the photo I D provided.

A copy of the photo ID will be obtained. Person performing customer due diligence will provide a signature verification stating the card was obtained in person and the ID supplied was reviewed in person. Refer to Appendix B, "Sample of New account Application."

Non-Face-to-Face Customers

When executing non –face- to face identification CAPOLIN applies tools based on artificial intelligence (AI) and machine learning (ML) . Using such tools allow CAPOLIN to conduct KYC based on reliable third party databases and software programs, as well as numerous offline and online data points from different channels, to create a holistic model of customer identity. It enables CAPOLIN to have more accurate and fast customer onboarding and verification process, less fraud and virtually no manual reviews.

In the case of customer due diligence performed in a non-face-to-face environment, such as online, verification will be conducted through one of the following methods, or a combination of methods;

Collection of a certified copy of a valid government-issued ID (see list outlined in the Face-to-Face section)

containing a photograph. Certification must be made by a notary public or attorney, and must include certifiers title, address, phone and fax number, license number and signature.

If a certified copy of the ID cannot be obtained, one of the following forms of ID is required (in addition to the uncertified copy of government-issued ID); and requiring additional documents to verify identity and address, which may include:

- An additional government-issued ID containing a photograph.
- Utility Bill.
- Tax assessment.
- Bank or credit card statement.
- Letter from public authority.
- Bank reference letter.
- Birth certificate.
- Requiring internet sign-on following verification procedures where the customer uses security codes, tokens, and/or other passwords which have been set up during card application and provided by secure delivery to the named individual at the independently verified address or email address.
- Communicating with the customer at an address that has been verified, such as direct mailing of card opening documentation which is required to be returned completed or acknowledged without alteration.
- Making Independent contact for the customer, for example by telephone at a number which has been verified prior to approving the card or conducting a transaction.
- Checking references with other institutions; or obtaining a financial statement.

At least two of the following data points will need to be confirmed when performing customer due diligence:

- Verify signature on physical application to signature on photo ID provided, when a physical application is collected.
- Verify the permanent address supplied to name by reviewing:
- Photo ID provided.
- Other document provided;
- Communicating with the customer at an address that has been verified, such as a direct mailing of card opening document, which in full or in part, might be required to be returned completed or acknowledged without t alteration; and verify data of birth supplied to name by reviewing:
- Verify ID number supplied to name by reviewing:

After obtaining the documents and information from customers and manually verifying the provided information according to the above mentioned points, all information should be uploaded in the operational IT system of CAPOLIN by respective employee and additionally verified using AL based verification tools and third party databases. The verification should include liveness checks, face, and photo liveness verification.

Business Customers

KYC/CDD for business customers requires collection and verification of the following:

- Name of cardholder (natural person); including full KYC/CDD.
- Name of corporate entity.
- Principal place of business and registered office.
- Mailing address.
- Contact telephone and fax number.
- Board resolution authorizing the opening of the card for each card holder.
- Certificate of Incorporation (original or certified copy, where applicable).
- Certificate of Good Standing,
- Certificate of Incumbency,
- Name, DOB, and address of all owners with over a10% interest.
- Name DOB, address of UBO/UBOs other than owners with over10% shares
- In the case of small businesses with a sole owner, or a sole proprietorship, KYC/CDD will be conducted on the owner as the natural person, providing that documentary proof can be provided verifying the corporate entity to the owner.

Comparison to Watch Lists

CAPOLIN's mandated KYC/CDD compliance includes determining whether the consumer appears on any list of known or suspected terrorists as provided by the relevant authorities, international sanctions lists, adverse media lists, etc.,.

Prohibited Customers

- CAPOLIN prohibits opening of card accounts for the following reasons/factors:
- Persons with addresses in Prohibited Countries or States List.
- Persons who are considered to be members of a criminal group, with suspicious; reputation, involved in criminal activities, fraud according to reliable sources and / or public information.
- Persons or entities, who are registered in non-cooperative jurisdictions.
- Persons who are engaged in weapon manufacturers, dealers, and intermediaries.

- Persons listed on the OFAC/UNSCR other relevant watch lists (see OFAC/UNSCR section.
- Persons listed on adverse media lists.

3.4.4. Record keeping.

CAPOLIN retains all customer identification records for six years after the last use of the account Information retained includes:

- Identifying information collected from the customer (name, address, DOB and ID number);
- Description of any non-documentary methods used, including results returned by the system.
- A copy or detailed description of any document used to verify identity (i.e. new card application, customer agreement).
- Description of the resolution for any substantive discrepancies discovered.

3.5. Know Your Partner/Partner Due Diligence (KYP/PDD)

Refer to Third Party Vendor Management for more details on the KYP/PDD process.

While CAPOLIN is responsible for performing the necessary due diligence and risk assessment of their Program Partners, issuing bank will have final approval.

3.5.1. Due Diligence

- CAPOLIN requires collection of the following information for each third-party provider:
- Name of the corporate entity and DBA name, I f applicable;
- Physical address of the headquarters and any branches;
- Mailing address;
- Tax identification number;
- Contact telephone number, email and corporate website;
- Name and address of all persons owning over 10% of the company;
- OFAC/UNSCR relevant other watch list check on the company and its owners and UBO's;
- Background checks of the company, owners, management and UBO's to ensure no involvement in illegal or prohibited activities;
- Description of primary business;
- Current business license, articles of incorporation, Certificate of Incorporation, Certificate of Incumbency, and Certificate of good standing (original or certified copy, where applicable);

3.5.2. Risk Assessment

CAPOLIN's Third-Party Vendor Management Policy outlines the risk assessment criteria and process for Third Parties. The risk assessment process considers the nine factors noted below. Each factor can be rated 1(low), 2(medium) or 3 (high)risk. The specific factors are:

- Company Structure.
- Country/State of Organization.
- Length of Time in Business.
- Primary Line of Business.
- Size of Business.
- Type of business
- Third Party Reputation/Background.
- Target Cardholders (if applicable).
- AML/CFT and sanctions Policies.
- UBO's
- PEP indicia, PEP associate indicia
- Consumer Complaints.

CAPOLIN also conducts risk-based monitoring of third parties to ensure compliance with applicable regulations as well as periodic due diligence reviews to ensure no material changes or weaknesses have occurred, or have developed, since the initial due diligence or previous review. The following factors will be considered in the periodic risk assessment:

- Company Structure.
- Country/State of Organization.
- Length of Time in Business.
- Primary Line of Business.
- Size of Business.
- Type of business
- Third Party Reputation /Background, including Consumer Complaints against entity.
- Location of the clients (if applicable).
- Marketing, Disclosures and Terms meet Brand Standards.
- Fraud Management.
- Suspicious Activity Referral.
- KYC; and Due Diligence– Beneficial Owners, PEP's, PEP's associates

3.5.3. Recordkeeping

All records relating to third party due diligence, approval, ongoing testing, as well as any communication regarding escalated or high-risk issues, are kept in electronic files. All records are kept for a period of six (6) years after termination of the third-party relationship.

3.5.4. AML/CFT Training

All third-party providers must provide proof of that they have been trained on AML/CFT policies and procedures. Proof of Training Records (prior to approval) need to include:

- Date of training;
- Name and title of the presenter;
- Attendee Names; and Copy of the training agenda or material covered.

3.6. Know Your Employer / Employee Due Diligence (KYE/EDD)

CAPOLIN may know that an insider can pose the same money laundering threat as a customer. It has become clear in the AML/CFT field that having equivalent programs to know your customer and to know your employee are essential.

A Know Your Employee (KYE) program means that CAPOLIN has a program in place that allows understanding an employee's background, conflicts of interest and susceptibility to fraud and money laundering complicity. Background screening of prospective and current employees, especially for criminal history, is essential to keeping out unwanted employees and identifying those to be removed.

The pre-employment background checks may:

- Reduce turnover by verifying that the potential employee has the requisite skills, certification, license, or degree for the position.
- Deter theft, fraud, and embezzlement.
- Prevent litigation over hiring practices.

Once the person is hired, an ongoing approach to screening should be considered for specific positions, as circumstances change, or as needed for a comprehensive review of departmental staff over a period of time.

Regularly repeated training of employees regarding what is expected from them should be part of normal on-the-job training.

Employees may be used to facilitate the laundering of funds; therefore, CAPOLIN must be alert to:

- An employee whose lavish lifestyle cannot be supported by his/ her salary.
- An employee who is reluctant to take a holiday or vacation when due.
- An employee who is associated with the mysterious disappearances or unexplained shortages of significant amounts of company funds.
- An employee who overrides internal controls or established approval authority or circumvents CAPOLIN's policy.

3.7. Transaction Monitoring

CAPOLIN in collaboration with the other financial institutions has adopted a policy for monitoring of suspicious activities. If suspicious activities are identified by CAPOLIN and/or its Processor, a Reportable Activity Referral (RAR) form will be completed.

CAPOLIN procedures regarding suspicious activity require:

- Monitoring of client, transaction, or prepaid cards for unusual or suspicious activity;
- Retain records of investigations and suspicious activity reporting for six years;
- Prompt reporting of any unusual or suspicious activity within one (1) business day of detection;
- Never "tip-off" a customer that they have been referred as a potential money laundering suspect or interfere with an investigation in to money laundering; and cooperating with any information requests or instructions received from the bank or any law enforcement agency, including requests to suspend or close card accounts.

3.7.1. Monitoring

CAPOLIN, through its Process, will conduct real time, or, if real time is not available, weekly monitoring of the clients transaction. CAPOLIN will be monitoring for, or systemically prevent, the following activity:

- Multiple transactions to the same person.
- More than seven cards or payment methods to the same address (not including apartment buildings);
- Merchant returns without off setting debits.
- High dollar value loads exceeding approved parameters.
- Transactions in restricted/blocked countries.
- Consistently high dollar value loads, withdrawals, or purchases, transactions defined as those exceeding approved parameters.

- Multiple value transactions within a certain period of time, from one source or different sources, that exceeds approved parameters; and More than 2 card accounts opened from the same IP address or multiple IP address changes.

3.7.2. Referrals

CAPOLIN acknowledges that RAR forms should also be filed on transactions that, although do not reach the requisite threshold amount, evidence possible violations or present indicia of possible money laundering.

CAPOLIN will file a RAR upon the discovery of:

Insider abuse involving any amount.

- Criminal violations aggregating $5,000 or more when a suspect can be identified.
- Criminal violations aggregating $25,000 or more regardless of a potential suspect.
- Transactions aggregating CAPOLIN knows, suspects, or has reason to suspect that the transaction is suspicious or does not comply with the business practice:
- Involves funds from illicit activities or is intended or conducted to hide or disguise illicit funds or assets as part of a plan to violate or evade any law or regulation, or to avoid any transaction reporting requirement under federal law or has no business or apparent lawful purpose or is not the sort of transaction in which that particular customer would normally be expected to engage, and CAPOLIN knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

Other transactions that potentially should raise "red flags," requiring further review and possible RAR filings include:

- Accounts, cards, or payment methods by many different persons with similar phone numbers, addresses.
- Many transfers to cards to one geographic area, transacted with in short period of time.
- accumulative totals that exceed normal location an individual, industry, or geographic area, etc.
- Unusual use of credit cards or debt instruments
- Unusually many credit card payments classified as “pre-authorization”
- The use of a personal/individual card account for business purposes or vice versa
- Card transfers are made in small amounts in an apparent effort to avoid triggering identification or reporting requirements
- Frequent card transactions involving round or whole dollar amounts purported to involve payments for goods or services.

- A dormant account suddenly becomes active without a plausible explanation
- Unusually frequent domestic and international automated teller machine (ATM) activity.
- Discovery that address and name are incorrect, fictitious or non-existent;
- Absence of conformity with recognized systems and controls

3.7.3. Record Retention Period

All records shall be retained for at least six (6) years. Scanned documents, micro film, microfiche or other commonly accepted forms of copying and retaining records are acceptable as long as the records are accessible within a reasonable period of time.

3.8. Sanctioned and Restricted Countries

CAPOLIN is prohibited from conducting business with, or approve cards for, entities or persons listed on the Sanctions lists published by OFAC, UNSCR. CAPOLIN will also not do business in any countries that are on UNSCR or Restricted Country List. This Policy Section has been established to meet OFAC/FATF/UNSCRS sanctions guidelines and mitigate other sanction risks.

3.8.1. Sanctions Screening Screening of New Customers

CAPOLIN will screen all applicants of the new accounts and all service providers and Program Partners against the sanctions lists published by OFAC, UNSCR , other relevant international watch lists, as well as CAPOLIN's Restricted Country List The screening of customers is a risk mitigating measure that needs to be embedded into the digital onboarding journey to identify if a customer is either on a sanctions list, or an individual that has been convicted for – or is suspected to be associated with – money laundering, the financing of terrorism or other financial crime.

Digital onboarding of such customers should be terminated upon confirmation that the customer is a sanctioned party and/or is connected to a sanctioned party; whereas mechanisms to ensure thorough review of "suspect" cases prior to proceeding to a next step in the account opening process should also be established. Accordingly, in the assessment of the technology solutions deployed for the purposes of onboarding, the screening mechanisms of customers and their connected parties are a vital consideration.

CAPOLIN uses IT-based monitoring systems to detect customers and transactions with conspicuous characteristics and to systematically abide by international financial sanctions and embargoes against certain persons, entities, and countries.

Ongoing Screening

Existing clients must be checked against the sanctions lists upon changes that take place in respective sanction, watch and other lists that are used by CAPOLIN, and/or up on implementation of new or modified CAPOLIN policies.

Validation and Reporting

CAPOLIN and/or their partners must document and enforce processes to determine whether an initial OFAC hit is a valid match or false hit. Valid hits are considered when:

Hit is a match to OFAC's SDN and other relevant international watch lists (Politically Exposed Person, FBI Most Wanted, and other control lists are not considered for Hits, and are considered for risk categorization of clients):

- Hit matches the name of the clients against an individual on the lists, and not matching an individual against a vessel, organization, or company, at least two pieces of the clients name matches the OFAC/UNSCR data, including aliases; or the complete SDN entry is compared against all of KYC/CCD of cardholder. If another piece of data matches in addition to the name match, this is considered a valid match.
- Clients with valid OFAC matches will be immediately suspended and reported for further instruction.

Record keeping

Records of OFAC violations and investigations must be held for 6 years.

3.8.2. Prohibited Countries

CAPOLIN will comply with instructions regarding its Restricted Country List. The list changes depending on number of factors , including, but not limited to:

- Sanctions programs established by OFAC and/or the United Nations.
- Countries designated as non-cooperative or of special concern by FATF.
- Countries that the Financial Services Regulatory Commissions have deemed to be Non-Cooperative or a "Watch Zone" list (Refer to Appendix E); and countries deemed by to be high risk based on the Bank's experience of past fraud/AML issues associated with the Country.
- Country is identified by credible sources as providing funding or support terrorist activities.
- Country is identified by credible sources as having significant levels of corruption or other criminal activity.
- Country with ties to terrorist organizations and / or the territory, which is bounded by the area controlled by the terrorists.
- Country is identified as a Conflict zone a place that is characterized by the serious instability, including military circumstances, armed conflicts, or activities of terrorist organizations.

- Country has been actively attracting funds for terrorist attacks.
- Country is widely known to have high levels of internal drug production or to be in drug transit regions.
- Country is considered as an offshore jurisdiction, offshore financial center, and tax haven.

For countries on the Restricted Country or UNSCR Sanctions List CAPOLIN is prohibited from:

- Doing business with companies in corporate in or trading in a restricted country.
- Doing business with individuals located in a restricted country.
- Doing business with nationals of a restricted country who are residents of a restricted country.
- Issuing or mailing cards to customers with an address in, or a government ID from, a restricted country.
- Allowing transactions to occur in a restricted country; and doing business with a partner organized in, or located in, a restricted country.

3.9. AML/CFT Training Program

CAPOLIN's Training Program is a cornerstone of CAPOLIN's commitment for preventing money laundering, financial crime (including bribery and corruption), terrorism financing, fraud, and other punishable acts. Strict compliance with the Training Program is a condition of employment for all employees. All employees are required to comply with the high standards set forth in the Training Program and are required to play an active role in preventing the use of CAPOLIN's services for illicit activities.

CAPOLIN AML/CFT training program provides initial and annual training to all staff, including Executive Management. The Executive Management will be informed of changes and new developments in the Compliance Program. While the Executive Management may not require the same degree of training as the operations personnel, they need to understand the importance of Compliance regulatory requirements, the ramifications of noncompliance, and the risks posed to the Company

Training program should cover.

- General concepts of ML/TF, Fraud, Financial Crime, corruption, bribery, and other criminal activities.
- General requirements of KYC/KYP/CDD/EDD principles.
- Typologies for client behavior or account movements that could indicate money laundering or terrorist financing.
- Relevant content of current Policy and other compliance related internal legal acts of the Company.

- Basic information about relevant applicable national legislations in the area of money laundering, terrorist financing.
- Basic information about client, Third party management policy.
- Employees' roles in the Company's compliance efforts and performance of respective duties.
- Updates of new laws, regulations and internal policies and procedures.
- Best practices and ML schemes.

Training records must include the date of training, name and title of the presenter, attendees and a copy of the training agenda or material covered. CAPOLIN will provide function specific training to employees regarding regulatory requirements and CAPOLIN 's internal AML/CFT policies and procedures. The training programs hall ensure that:

All employees, including senior management, who have contact with customers (whether in person or by phone), who see customer transaction activity, or who handle cash in any way, or whose professional tasks include establishing business relationships, carrying out payment transactions or acquiring merchants receive appropriate training.

Upon starting their tenure with CAPOLIN, all employees must be informed about strategy for anti-money laundering and counter terrorism financing as well as the prevention of financial crimes or other punishable acts.

All employees of CAPOLIN must participate in AML training within the three months of their tenure. Follow up AML training must be provided at least bi-annually.

Training is ongoing and incorporates current developments and changes to anti-money laundering laws and regulations; new and different money laundering schemes involving customers and stored value are addressed.

The program provides guidance and direction related to non-compliance with CAPOLIN's AML/CFT policies or violation of law; no person connected with CAPOLIN shall counsel or instruct customers on" structuring" transactions. Employees who assist or willfully ignore customer efforts to avoid filing and reporting requirements violate the law and may be subject to criminal penalties, possible in cancelation, and civil fines.

CAPOLIN has adopted a "zero tolerance" policy subjecting employees to immediate dismissal for any such violations; and all persons and entities, including employees and contractors found to violate the provisions of the AML/CFT will be summarily reported to the appropriate authorities.

4. Independent Testing

The primary purpose of the independent testing/review is to monitor the adequacy of CAPOLIN's anti-money laundering program. The review should determine whether the business is operating in compliance with the requirements of the laws and regulations, international standards and CAPOLIN's own policies and procedures

CAPOLIN AML/CFT program tests all of its programs for their effectiveness annually. This testing can be done by an independent party, either internal or external. If internal, the person(s) conducting the review must be independent from the designated AML/CFT Officer and staff, and must have enough knowledge of AML/CFT requirements to adequately perform the testing.

The review should provide a fair and unbiased appraisal of each of the required elements of anti-money laundering program, including policies, procedures, internal controls, recordkeeping and reporting functions, and training. The review should include testing of internal controls and procedures to identify problems and weaknesses and, if necessary, recommend to Executive management appropriate corrective actions.

- Testing includes review of the following elements:
- AML/CFT Risk Assessment.
- Four Pillars of the AML/CFT Compliance Program:
- Policies, Procedures, and Internal Control.
- Designated Compliance Officer and
- Independent Review.
- AML/CFT Training.
- Transaction Monitoring–Currency Transaction and RAR filings.
- OFAC& UNSCR Sanction.

Customer Identification Program &Customer Due Diligence.

5. Reporting

Monthly reporting (with support of processor reporting):

- Number of Card holder accounts opened during the month.
- Number and reason of customer applications declined during the month.
- Number of total open and active customer card accounts.
- Number of total open and inactive customer card accounts.
- Top10 countries by card holder volume =only issued cards.
- Number of Open Investigations at month-end on customer card accounts.
- Number of False Positives investigated.
- Number of Unusual Activity Referrals (Reportable Activity Referrals) made for the month.
- Charge back Tracking Logs.
- Fraud Case/Exception Item Tracking Logs.
- Dispute Tracking Logs; and total number of alerts processed in the month:

Alert Type	Count
Alert from Load Approval Dept.	
Alert from partner	
Alert from CAD	
Alert from CS	
Shared Card Usage	
Load Monitoring Alerts	
Grand Total	

Additionally, Compliance Officer is responsible for appropriate reporting on the results of his/her activities. A summarized report shall be given to the Executive Management on a quarterly basis laying out details on number(s) of:

Transactions executed by risk category of customers; a statistical analysis of the development of the risk categories of customers; number and amount of rejected transactions and business relationships, and their brief description; investigations on suspicious transactions together with the results of such investigations and reasons for suspicion; information regarding to PEPs and on any unusual observations regarding their behavior; number of true hits of customers and client database in regards with Sanctions screenings;

General observations relevant to the AML/CTF activities.

Appendix A: Sample of New Prepaid Card Application

Know Your Customer/Customer Due Diligence Worksheet

Note: Important Information for Approving a New Card

To help fight money laundering activities, please obtain, verify, and record information that identifies each person who applies for a prepaid card. Ask for name, address, date of birth, and other information to identify the cardholder.

Customer Legal Name:	
Physical Address(cannot be a PO Box):	Mailing Address(can be a PO box):
Date of Birth:	Country of Birth:
Nationality:	Purpose of Card:
Phone Number:	Email:
Identification Type:	ID Number:
Issuing government(state or country):	Issuance date:
	Expiration date:

I hereby acknowledge receipt of the notice on this form and state that all of the identifying information I have provided is current and accurate.

(Signature of Customer) Date

For Program Partners Only:

By signing below, you confirm you approved this card in person and were presented, by the prospective customer, with a validly issued government identification document containing a photograph. Copy of said ID is attached to this record. You confirm verification of two (2) of the following:

□Signature and Photo Likeness	□Address to Name; if further documentation was collected to verify address please note what type:		
□Utility bill	□Tax assessment	□Letter from public authority	
□Bank or credit card statement	□Date of Birth to Name	□Other_____	
□ID Number to Name			
Signature of Reseller:		Date:	
Card Number:		Program Name:	

Appendix B: Reportable Activity Referral (RAR)

Partner Information	
Company Name:	
Referral Completed by:	
Contact Phone Number:	
Contact Email:	
Referral Details:	
Date of Referral:	
Has Law Enforcement been notified?	
If yes, what Agency?	
If yes, Name and Phone number of Person Contacted:	

Subject/SuspectInformation(attachadditionalsheetsifmultiplesubjects)	
Subject Name:	
Subject Address:	
Subject Card Account Number:	
Subject Relationship: (customer employee ,partner, etc.)	
Subject Phone Number:	
Subject Email:	
IP Address Involved:	
Subject Identification Number:	
Subject Date of Birth:	
Subject Occupation:	
Form of Identification on File for Subject:	
Issuing Authority:	
ID Number:	

Details of Suspicious Activity or Transactions	
Date or date range of activity:	
Date first detected:	
Total Dollar Amount Involved:	
Amount of Loss:	
Amount of Recovery:	

Detailed Narrative

Appendix D: Restricted Country List

As of December 2015, the countries below, make up Restricted Country List:

Afghanistan	Heardand McDonald Islands	North Korea
Bhutan	India	Papua New Guinea
British Indian Ocean Territory	Iran	Solomon Islands
Christmas Island	Kiribati	Sri Lanka
Cocos(Keeling)Islands	Macau	Syria
Cook Islands	Nauru	Tokelau
Cuba	New Caledonia	Tonga
Fiji	Niue	Tuvalu
French Polynesia	Norfolk Island	Vanuatu
Guam		

For any country on the list, CAPOLIN will not:

- Do business with any companies, incorporated in or trading in a restricted country.
- Do business with individuals located in a restricted country.
- Do business with nationals of a restricted country who are resident of that restricted country.
- Issue or mail cards to customers with an address in, or a government ID; from, the restricted country.
- Do business with a partner organized In, or located in, a restricted country; or allow transactions to occur in the restricted country.

Appendix E: "Watch Zones"

On Establishing the List of Watch Zones for the Purpose of the Laws of the United States "On Facilitating the Prevention of Illicit Income Legalization"

Pursuant to The Office of National Drug and Money Laundering Control Policy Act, 2003 of the United States and in conjunction with Bureau of International Narcotics and Law Enforcement Affairs March2018 International Narcotics Control Strategy Report (INCSR) of the United States, Volume II page 49 Countries of Primary concern, I decree:

Approve the List of Watch Zones pursuant to the Law of the United States on Facilitating the Prevention of Illicit Income Legalization:

Afghanistan	Antigua and Barbuda	Argentina
Australia	Austria	Bahamas
Belize	Bolivia	Brazil
British Virgin Islands	Burma	Cambodia
Canada	Cayman Islands	China, People Republic
Columbia	Costa Rica	Curacao
Cyprus	Dominican Republic	France
Germany	Greece	Guatemala
Guernsey	Guinea Bissau	Haiti
Hong Kong	India	Indonesia
Iran	Iraq	Isle of Man
Israel	Italy	Japan
Jersey	Kenya	Latvia
Lebanon	Liechtenstein	Luxembourg
Macau	Mexico	Netherlands
Nigeria	Pakistan	Panama
Paraguay	Philippines	Russia
Singapore	Somalia	Spain
St. Maarten	Switzerland	Taiwan
Thailand	Turkey	Ukraine
United Arab Emirates	United Kingdom	United States
Uruguay	Venezuela	Zimbabwe

1. The Financial Services Regulatory Commissions of each Country shall be asked to verify annually (at least once a year) the List of Watch Zones and in necessity of changes to the list shall present the relevant information to CAPOLIN.

3. The present Decree shall become effective on the15th day following its promulgation.

Appendix G: Glossary of Terms

Anti-Money Laundering (AML) – A term mainly used in financial services to describe regulatory controls that require financial institutions and other regulated entities to prevent or report money laundering activities.

Card Network/Association – A network of issuing banks and acquiring banks that process payment cards of a specific brand such as MasterCard, Visa, and Union Pay.

Card Program(s)–Refers to Prepaid Card Program (s) managed by CAPOLIN.

Cardholder–The person to whom a prepaid card is issued.

Card Issuer– A financial institution that issues prepaid cards.

CAO–Chief Administrative Officer

CCO–Chief Compliance Officer.

CDD–Customer Due Diligence.

CRO–Chief Risk Officer.

CSR–Customer Service Representative.

FCU - Financial Compliance Unit created an act to amend the Office of National Drug and MoneyLaundering Control Policy Act of 2008. This required institutions to have mandatory AML/CFT policies and procedures that will deter and detect money laundering. These institutes have to be able to recreate transaction records for further review against the law and possible criminal procedures.

Issuing Bank – A financial institution that acts as a sponsor for CAPOLIN in offering card associationbranded payment cards to consumers. It is the Issuing Bank's responsibility to ensure compliance of card association rules and applicable government regulations through hits requirements of CAPOLIN.

Identification of person – obtaining information on the person, which, when necessary, allows tracing such person and distinguishing from other person.

Verification-evidence that establishes or confirm accuracy or truth of something.

KYC–Know Your Customer.

Non-Cooperative/Watch Zone – A country or a part of the territory thereof defined by the CentralBank of the Country where CAPOLIN will be conducting business on the basis of proposition of the Financial Monitoring Service of those countries. The country or territory thereof shall be identified as such on the basis of the information provided by competent international organization, or if the grounded supposition exists that in such zone weak mechanisms for controlling illicit income

OFAC – Office of Foreign Assets Control - A department of the U.S. Treasury that enforces economic and trade sanctions against countries and groups of individuals involved in terrorism, narcotics, and other disreputable activities.

UNSCR – United Nations Security Council Resolutions. The UNSCR Sanctions Committee issues economic and trade sanctions against countries and groups of individuals involve d in terrorism, narcotics, and other disreputable activities.

Reportable Activity Referral (RAR) - A form used by CAPOLIN to refer possible suspicious activity for further investigation which may lead to submitting a Suspicious Transaction Report (STR) with the Financial Monitoring Service of each Country CAPOLIN operates.

Subject Matter Expert (SME) – Individual assigned responsibility for the policy and/or related procedures.

Suspicious Transaction Report (STR) – If a reporting entity suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity or are related to terrorist financing, it shall, as soon as possible but no later than 3 business days, report promptly its suspicions to the Financial Intelligence Unit(FIU).

Third Parties – Entities with which CAPOLIN has business relationships in order to deliver its Card Programs which includes Program Partners and Service Providers/Vendors.

Appendix H: Financial Action Task Force(FATF) Guidance

The FATF Guidance identifies the following "unique" risks to prepaid access:

The FATF has developed a series of Recommendations that are recognized as the international standard for combating of money laundering and the financing of terrorism and proliferation of weapons of mass destruction. They form the basis for a coordinated response to these threats to the integrity of the financial system and help ensure a level playing field. First issued in 1990, the FATF Recommendations were revised in 1996, 2001, 2003 and most recently in 2012 to ensure that they remain up to date and relevant, and they are intended to be of universal application.

Non-face-to-face relationships and anonymity: non-face-to-face contact may indicate a higher risk, due to factors such as impersonation fraud, or money laundering/terrorist financing. The FATF Guidance notes that the risk posed by anonymity may occur at purchase, registration, loading, reloading, or customer use. The FATF Guidance states the level of risk is relative to the functionality of the prepaid access; Funding - The FATF Guidance notes that funding of prepaid may occur in various ways with differing degrees of customer due diligence. The FATF Guidance is especially concerned with cash funding, which may be fully anonymous, and the ability to pass prepaid cards on to third parties. The FATF Guidance first notes that prepaid access reduces the incentives for providers to conduct comprehensive customer due diligence because credit risk is absent. Afurtherriskassociatedwithprepaidaccessfundingincludesreloadabilitywithnolimits;

Geographical Reach - The FATF Guidance pays particular attention to open-loop prepaid access in examining this risk because those products often enable customers to make payments at both domestic and foreign points of sale. Additionally, the FATF Guidance notes that some prepaid access programs allow customers to make person-to-person transfers and that the compact physical size of the cards themselves increase their vulnerability because criminals may use them – in lieu of cash – to make cross-border transportations of value. The FATF Guidance highlights prepaid access ability to access funds internationally as being particularly vulnerable. Such vulnerability stems from the logistical benefits of transporting prepaid access with accounts loaded with high value, not determinable from the prepaid access itself.

Access to Cash - The FATF Guidance expresses concerns over the risk of access to cash through international automated teller machine ("ATM") networks. Such access increases the level of money laundering and terrorist financing risk, and may be either direct, through prepaid access, or indirect, through mobile and internet payments interconnected with prepaid access; and segmentation of Services - A final risk identified by the FATF Guidance is the number of parties involved in providing prepaid access. Such risks include (1) the large number of parties increases the danger of losing customer or transaction information and that (2) prepaid access providers will rely on agents and unaffiliated Third-Party Agents to establish customer relationships and reload funds. Further, the FATF Guidance notes that entities providing prepaid access may come from sectors unfamiliar with AML controls