AML Policy

Effective Date 25/10/2023

The Policy applies to all Primeon Payments Limited employees, all units in the Primeon Payments Limited, senior management, foreign correspondents, contractors, and third parties with whom Primeon Payments Limited may contract.

The purpose of Primeon Payments Limited is not only to comply with relevant legal requirements, but also to mitigate and reduce the potential risk to Primeon Payments Limited of our customers using our products, services, and delivery channels to launder the proceeds of illegal activity, fund terrorist activity, or conduct prohibited financial sanctions activity.

The Policy is updated at least once a year, or more frequently based on international requirements and legislative changes, particularly with the implementation of the Canadian Payments Act, Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), or Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTF Regulations) and associated regulations or Financial Transactions and Reports Analysis Centre (FINTRAC) Guidance on the Risk-Based Approach and Compliance program requirements.

Contents of the Policy

DEFINITIONS

1. “AML Policy” – the Anti-Money Laundering Policy;
2. “CDD” – Customer Due Diligence;
3. “CSIS” – Canadian Security Intelligence Service;
4. “CTF” – Counter-Terrorism Financing;
5. “EDD” – Enhanced Due Diligence;
6. “EU” – European Union;
7. “FATF” – Financial Action Task Force;
8. “FinCEN” – The Financial Crimes Enforcement Network;
9. “FINTRAC” – Financial Transactions and Reports Analysis Center;
10. “KYB” – Know Your Business;
11. “KYC” – Know Your Customer;
12. “MSB” – Money Service Business;
13. “Nominated Officer” – A Nominated Officer (also known as the MLR officer or AML Compliance Officer) is the focal point within the company for the oversight of all activity related to anti- financial crime issues;
14. “OFAC” – Office of Foreign Assets Control;
15. “PCMLTFA” – Proceeds of Crime (Money Laundering) and Terrorist Financing Act;
16. “PEP” – Politically Exposed Persons;
17. “RCMP” – Royal Canadian Mounted Police;
18. “STR” – Suspicious Transaction Report;
19. “Supporting Officer” – A person or persons nominated to act on behalf of the Nominated Officer;
20. “SWIFT” – Society for Worldwide Interbank Financial Telecommunications;
21. “UBO” – Ultimate Beneficial Owner;
22. “UN” – The United Nations.

Primeon Payments Limited (also referred to as the “Company”) has formulated an AML Policy that aligns with statutory requisites and embodies guidelines for effectively managing risks associated with money laundering and terrorist financing within the organization.

Registered as a Money Service Business (“MSB”) with the Financial Transactions and Reports Analysis Centre of Canada (“FINTRAC”), Primeon Payments Limited commits to full cooperation with FINTRAC and other law enforcement entities in their endeavors to uncover, prevent, and deter instances of money laundering and terrorist financing.

MITIGATION OF MONEY LAUNDERING & TERRORIST FINANCING IN CANADA

Money laundering involves activities intended to disguise or cloak the true origins of illicitly obtained proceeds, making them appear to stem from lawful sources or consist of legitimate assets. It also encompasses funds, regardless of their acquisition, being utilized for sponsoring terrorism. Terrorist financing may not necessarily involve proceeds from criminal activities but instead aims to conceal the source or intended use of funds, which may later be employed for illicit purposes.

The laundering of money typically progresses through three key stages, often entailing multiple transactions. An MSB should be vigilant for signs indicating potential criminal activities.

These stages comprise:

1. Placement: Illegally generated cash is converted into monetary instruments like money orders or traveler’s checks, or deposited into accounts at financial institutions.
2. Layering: Funds are transferred or channeled into alternative accounts or financial institutions to further detach them from their illicit origins.
3. Integration: Reintroducing funds into the financial system for purchasing legitimate assets or funding other criminal activities or lawful enterprises.

Upon successful layering, integration strategies effectively reintegrate laundered funds into the wider financial framework, presenting them as outcomes of, or connected to, genuine business operations.

Terrorist financing pertains to acquiring or possessing funds (directly or indirectly) with the intent for them to support actions defined as terrorist acts or for disposal to a terrorist group or individual.

Proliferation financing denotes the provision of funds or financial services, either wholly or partly, to manufacture, procure, possess, develop, export, transit, broker, transport, transfer, stockpile, or deploy nuclear, chemical, or biological weapons and related materials (comprising technologies and dual-use goods utilized for non-legitimate purposes), in violation of national laws or, where relevant, international commitments.

Proceeds from criminal activities constitute criminal property, encompassing any form of conduct – regardless of location – that would amount to a criminal offense if perpetrated within Primeon Payments Limited. This encompasses drug trafficking, terrorist acts, tax evasion, corruption, fraud, forgery, theft, counterfeiting, blackmail, and extortion, along with any other offenses committed for monetary gain.

Primeon Payments Limited has instituted its AML Compliance Policy to effectively address and mitigate identified money laundering risks. This necessitates implementing robust systems and controls to diminish the likelihood of the company being exploited to facilitate financial crimes. This program is crafted to embody the fundamental tenets of Anti-Money Laundering and Combating Terrorism Financing practices and norms, to be strictly adhered to by Primeon Payments Limited.

The AML Policy is grounded in relevant AML legislation, regulations, and official directives from the Government of Canada. Furthermore, it is tailored to align with the Financial Action Task Force (FATF) Standards regarding combatting money laundering, terrorism financing, and proliferation.

AML SYSTEMS

The primary legislation overseeing AML in Canada is the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), accompanied by the PCMLTF Regulations, which detail specific requirements, including:

- the designation of an individual responsible for overseeing the compliance program;
- the formulation and enforcement of up-to-date compliance policies and procedures endorsed by a senior officer;

- a framework to evaluate the risk of potential money laundering or terrorist financing activities within the organization, along with measures to mitigate high-risk scenarios;
- a continuous written compliance training program for employees of Primeon Payments Limited;
- a biennial review of policies and procedures to assess their efficacy, to be conducted by either an internal or external auditor.

The PCMLTFA and the most recent iteration of FATF recommendations mandate relevant businesses to develop and uphold suitable, risk-centric policies and procedures related to:

- Customer due diligence
- Reporting
- Record-keeping
- Internal control
- Risk assessment and management (Risk Based Approach)
- Monitoring and managing compliance
- Internally disseminating these policies and procedures to prevent potential money laundering, terrorist financing, and proliferation financing activities. These policies and procedures should:
- Identify and scrutinize:
    - Complex or exceptionally large transactions
    - Unusual transaction patterns lacking clear economic or lawful justification
    - Any other activities suggesting links to money laundering, terrorist financing, or proliferation financing
- Define additional measures to deter the use of products and transactions that enable anonymity in money laundering or terrorist financing schemes
- Determine if a customer qualifies as a politically exposed person
- Appoint an individual within Primeon Payments Limited to ensure compliance with and receive disclosures under the PCMLTFA and associated Regulations.
- Encourage employees to report suspicious activities to the designated officer, who must evaluate internal reports against available information to assess knowledge or suspicion of money laundering or terrorist financing.

The foundational principles of the PCMLTFA and associated Regulations, embodying a Risk-Based Approach (RBA), entail a series of actions to identify the most cost-effective and proportional strategies to manage and mitigate money laundering, terrorist financing, proliferation financing, and sanctions violation risks encountered by the business. These actions involve:

1. Recognizing relevant money laundering, terrorist financing, proliferation financing, and sanctions violation risks;
2. Evaluating risks posed by:
    - Various customer types and behaviors
    - Assortment of products and services
    - Different delivery channels, such as cash transactions, electronic transfers, wire transfers, or checks
    - Geographical operating regions, including business premises location and sources or destinations of customer funds
    - Complexity and volume of transactions;
3. Establishing and executing measures to control and minimize these identified risks;
4. Monitoring and enhancing the efficacy of these controls;
5. Documenting actions taken and the rationale behind them.

To ensure the proper implementation of AML procedures and controls, Primeon Payments Limited has established effective controls that encompass:

- A robust AML compliance program
- Oversight by senior management
- Appointment of a Compliance Officer / Money Laundering Reporting Officer (MLRO)
- Compliance and audit function
- Staff screening and training.

Primeon Payments Limited places great importance on maintaining a reputation for integrity and transparency in its business model and management systems and procedures. Upholding these standards is integral to the company's commercial objectives, corporate responsibilities, and adherence to high standards of Anti-Money Laundering and Combating Terrorism Financing (AML/CTF) measures. The company aligns with

established international standards to prevent any misuse of its services for the aforementioned purposes.

THE MONEY LAUNDERING REPORTING OFFICER (NOMINATED OFFICER)

The Nominated Officer, designated within an organization, assumes the responsibility for overseeing all matters pertaining to anti-money laundering practices. Primeon Payments Limited's Nominated Officers must stay abreast of AML regulations and risks. If Nominated Officers are extensively involved in daily regulatory tasks and amendments to AML requirements, they may require additional support to effectively oversee an AML regime. In such cases, Primeon Payments Limited may consider appointing a suitably qualified individual as the Nominated Officer.

The responsibilities of the Nominated Officer entail:

1. Receiving disclosures from employees (referred to as Suspicious Transaction Reports - STRs).
2. Determining whether disclosures should be reported to the Financial Transactions and Reports Analysis Centre, the Royal Canadian Mounted Police, or the Canadian Security Intelligence Service.
3. Monitoring new regulations and assessing their impact on the company's operational processes.
4. Establishing a written procedures manual accessible to all staff and stakeholders.
5. Ensuring thorough due diligence on customers and business partners.
6. Receiving internal Suspicious Transaction Reports from staff.
7. Deciding which internal STRs should be reported to FINTRAC, the RCMP, or CSIS.
8. Appropriately documenting decisions related to STRs.
9. Ensuring that staff receive anti-financial crime training upon joining and regular refresher training.
10. Monitoring business relationships, recording reviews and decisions made.
11. Deciding on the continuation or termination of trading activities with specific customers.

12. Ensuring all business records are retained for a minimum of five years from the last customer transaction, as per FINTRAC regulations.

The Supporting Nominated Officer steps in when the Nominated Officer is unavailable.

STAFF TRAINING

Primeon Payments Limited maintains an ongoing employee training program to ensure staff is proficient in Know Your Customer (KYC) procedures and is knowledgeable about various money laundering patterns and techniques that may arise in their daily operations. Training focuses differ for new staff, front-line staff, compliance staff, and those engaging with new customers or Merchants. New staff members receive education on the significance of KYC policies and essential Company requirements.

Training is provided to all staff upon joining Primeon Payments Limited and regularly thereafter (at least annually). Customer-facing staff are trained to verify new customers' identities, conduct due diligence on existing customer accounts continuously, and identify suspicious activity patterns. The training also covers obligations stemming from external (legal and regulatory) and internal requirements, alongside specific duties to be followed in daily operations and recognition of money laundering, financial crime activities, or sanctions violation typologies.

Regular refresher training is conducted to reinforce employees' responsibilities and apprise them of any updates. It is vital for all relevant staff to comprehend and consistently implement KYC policies. Fostering an organizational culture that promotes this understanding is key to successful implementation.

Training encompasses the following topics:

1. Applicable laws on financial crime.
2. Risks associated with financial crime threats to the company.
3. Role and responsibilities of the Nominated Officer.
4. Internal policies and procedures.
5. Customer Due Diligence/Enhanced due diligence monitoring measures.

6. Identifying suspicious activity indicators.
7. Submitting internal Suspicious Transaction Reports to the Nominated Officer.
8. Record-keeping requirements.
9. Recognizing potential sanctions violations.

The Nominated Officer maintains a training log for all staff training sessions. Staff members are required to sign the training log when necessary to confirm receipt of training. The Nominated Officer disseminates additional materials to raise awareness of anti-financial crime issues among all staff, which should be displayed on the company notice board accessible at all company locations. The Nominated Officer includes information about attended education and training programs in their Annual Report. Primeon Payments Limited utilizes training programs offered by the Canadian Anti-Money Laundering Institute for internal training updates. Additionally, the Company leverages learning resources from reputable organizations like ACCP, ACAMS, and ICA.

CUSTOMER DUE DILIGENCE (CDD/KYC)

Customer due diligence (CDD) is a cornerstone of a robust anti-money laundering and counter-terrorism financing (AML/CTF) framework. Primeon Payments Limited is committed to identifying and verifying each customer to:

- Assess the money laundering and terrorism financing risk associated with each customer.
- Determine the course of action regarding business relationships or transactions.
- Evaluate the level of ongoing monitoring required.

Primeon Payments Limited has instituted a Know Your Customer (KYC) program to subject all customer types to comprehensive identification, risk assessment, and monitoring measures. This program is uniformly applied across all divisions of Primeon Payments Limited to mitigate the risk of the company being utilized for illicit financial activities. Multiple online databases containing individual and business information are utilized to verify all customer/client identification details before activating a e-account.

Prior to engaging with a new customer or initiating a transaction with a customer where a well-established relationship does not exist, Primeon Payments Limited undertakes thorough due diligence to ensure confidence in the integrity of customers and the legality of proposed transactions. This includes:

1) Making reasonable efforts to ascertain the true identity of all customers and the legal and beneficial ownership of accounts.
2) Determining customer citizenship, residential and business addresses, occupation, or business type, and obtaining supporting documentation as needed.
3) Verifying whether the customer holds sole interest in the account or if others have access, and conducting due diligence on these individuals.
4) For non-individual customers:
   - Determining the legal entity status (e.g., corporation, partnership).
   - Assessing whether the customer is regulated domestically or internationally.
   - Identifying all key individuals of the customer, such as officers, directors, or substantial beneficial interest holders (i.e., those owning 25% or more of the company). Primeon Payments Limited ensures that corporate and legal entities incorporated within their jurisdiction maintain accurate and current information on beneficial ownership, including details of beneficial interests held.
   - Obtaining relevant organizational documents:
   - Following pre-approval for processing, employees gather a comprehensive documentation package via email and forward it to the Primeon Payments Limited Compliance Team and Acquirer Bank, including:
   • Company registration documents issued in the country of incorporation (e.g., Certificate of Registration, Articles and Memorandum, Certificate of Registered Address, Certificate of Directors).
   • Ownership rights documents of the ultimate beneficial owner (e.g., Shareholder Certificate, Share Transfer, eRegister).
   • Identification documents with the holder's signature (e.g., ID Card, Passport).

- Representation rights documents for the company (e.g., Power of Attorney, Articles, Minutes of Meeting).
- Partner and supplier agreements, if applicable.
- Licenses, if applicable.
- Financial statements, if applicable.
- Processing history, if applicable.

5) Identifying the source of customer funds.
6) Conducting screenings for:
   - Matches on the OFAC list.
   - Global Affairs Canadian sanctions list.
   - Persons holding significant equity (>25%) in a business are subject to AML/CTF screening.
7) Ascertaining the frequency of customer fund transfers and third-party payments to or from the account, where applicable.
8) Obtaining and contacting reputable references, such as professionals and financial industry members, banks, or securities companies.
9) Government Officials and Foreign Bank Accounts:

   Specific procedures are applied for politically exposed persons (PEPs) and accounts opened by or through foreign banks or high-risk client countries or industries. Primeon Payments Limited implements enhanced and ongoing due diligence measures commensurate with customer risk levels. High-risk customers undergo enhanced due diligence processes, with ongoing reviews based on their risk categorization (high, medium, or low).

10) Accounts through an Intermediary:

    In cases where accounts are intermediated, the Agent must conduct due diligence on the account or ensure that the intermediary has performed satisfactory due diligence aligned with the Agent's “Know Your Customer” policy.

    - Due diligence scope varies based on historical relationships with the intermediary, regulatory status of the intermediary, and jurisdiction. The Compliance Officer should guide the requisite due diligence for a specific intermediary.
    - At a minimum, due diligence on an intermediary should include reviewing their anti-money laundering and counter-terrorism

financing procedures. Representation from the intermediary regarding compliance with their procedures may be sought.

- Reference checks through trusted sources should be conducted for intermediaries not regulated or lacking known anti-money laundering and counter-terrorism financing procedures.

11) Counterparties

The guidelines outlined above for intermediaries also apply to transactions with counterparties acting on behalf of customers. Counterparties include private transaction parties, banks, dealers, agents, and intermediaries. While limited due diligence suffices for regulated counterparties in jurisdictions with robust anti-money laundering and counter-terrorism financing regulations, non-regulated counterparties require similar due diligence as clients.

ENHANCED DUE DILIGENCE (EDD)

Primeon Payments Limited employs Enhanced Due Diligence to address situations where the customer and product/service combination pose heightened risks. This escalated level of due diligence is essential to mitigate the amplified risk. High-risk scenarios typically arise when there is a heightened susceptibility to money laundering or terrorist financing through the services and products offered by Primeon Payments Limited or involving a customer of the Company.

The specifics of enhanced due diligence procedures vary based on the nature and severity of the risk.

1. High-risk situations

In circumstances inherently carrying a higher risk of ML/TF, Primeon Payments Limited implements additional measures to mitigate these risks effectively.

Enhanced due diligence measures may include:

- Gathering additional information on the customer (e.g., related parties, accounts, relationships) and updating customer profiles, including identification data, more frequently.
- Acquiring further details on the planned nature of the business relationship (e.g., anticipated account activity), source of wealth, and source of funds.
- Obtaining senior management approval to initiate or continue the relationship.
- Intensifying monitoring of the business relationship by enhancing control frequency and timing and identifying transaction patterns requiring further scrutiny.

2. Source of Wealth vs Source of Funds

Verifying the customer's source of wealth or source of funds is a fundamental aspect of EDD. Source of wealth refers to the origin of the individual's total wealth, providing insights into the individual's wealth scale and acquisition methods. While specifics about assets not handled by Primeon Payments Limited may be unavailable, general information can be gathered from individuals, commercial databases, or other open sources.

Source of funds pertains to the origin of specific funds or assets involved in the business relationship between an individual and Primeon Payments Limited. This includes funds being invested, deposited, or wired as part of the relationship, encompassing the activity generating these funds. The information obtained should be substantive, establishing the provenance or rationale behind the acquisition of funds.

3. Politically Exposed Persons (PEPs)

In an effort to reduce potential risks, Primeon Payments Limited conducts Enhanced Due Diligence at the onset of a business relationship and maintains ongoing monitoring upon discovering or suspecting a business relationship with a PEP.

The definition of “PEP” includes individuals who: currently or within the past year have held significant public roles; are immediate family members of such individuals; are known associates of such individuals; are residents outside or within the specified jurisdictions; have been entrusted with prominent

public functions by any state, the European Community, or an international body, or are immediate family members or close associates.

When a PEP is identified:

- Senior management approval must precede the establishment of a business relationship with a PEP.
- Verification of the source of funds is crucial.

Before engaging in a business relationship with a PEP, verifying the source of funds is imperative. Primeon Payments Limited must ensure that there are no signs indicating that funds for transactions derive from corrupt activities, fraud, or an attempt by the PEP to conceal assets. Establishing the source of funds from the PEP may involve a series of questions to determine their income sources, business interests, and investments.

It is noted that Primeon Payments Limited does not currently conduct transactions with any PEPs.

RISK-BASED APPROACH (RBA)

1. Risk assessment and risk categories

The Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and its Regulations aim to detect and deter money laundering and terrorism financing. Introduced in 2008, amendments to the PCMLTFA and its Regulations strengthened the Canadian anti-money laundering and anti-terrorism financing (AML/ATF) regime. As part of these amendments, the Risk-Based Approach (RBA) mandates reporting entities to assess their exposure to money laundering and terrorism financing risks based on prescribed criteria.

Risk may be determined through objective and subjective criteria, assigning a “risk rating” to each criterion.

As part of its AML Program, Primeon Payments Limited has conducted a risk analysis to pinpoint potential money laundering risks. This approach involves identifying money laundering and terrorism financing risks of customers, customer categories, and transactions to implement appropriate measures and controls. Monitoring customer transactions and conducting ongoing

reviews are integral to Primeon Payments Limited's risk-based approach. This risk assessment process can be tailored for specific customers based on information received from competent authorities.

Money laundering and terrorism financing risks at Primeon Payments Limited are classified into the following categories for effective risk management:

- Low Risk: Easily identifiable entities with transparent sources of wealth and conforming transactions.
- Medium Risk: Customers posing higher-than-average risks due to backgrounds, activities, locations, and sources of funds.
- High Risk: Customers requiring enhanced due diligence measures, especially those with unclear sources of funds. Enhanced due diligence is applied to all high-risk customers, guided by specific criteria such as high-risk jurisdictions, complex structures, or involvement in restricted activities.

Primeon Payments Limited deems the following customer categories as high risk:

- High Net Worth Individuals
- Trusts, charities, NGOs receiving donations
- Companies with close family shareholding
- Politically Exposed Persons (PEPs) from foreign origins
- Non-face-to-face customers
- Companies issuing bearer shares
- Businesses involved in oil products trade or new financial products
- Entities with dubious reputations based on available public information

Country Risk Assessment

Country risk analysis, in conjunction with other factors, provides insights into potential money laundering and terrorism financing risks. Factors contributing to higher risk include countries under sanctions, lacking AML regulations, and supporting terrorist activities.

Primeon Payments Limited considers jurisdictional risks based on customer and beneficial owner locations, principal business sites, and personal associations. The company maintains lists of non-cooperation countries and

high-risk jurisdictions, aligning with reputable sources like international bodies, AML indices, and sanctions programs.

Customer Risk Evaluation

Assessing potential money laundering and terrorist financing risks posed by customers is crucial. Based on identified criteria, Primeon Payments Limited determines elevated risks and applies appropriate mitigation strategies. Elevated risk indicators include unusual transactions or structures complicating identification of true owners. The Company also evaluates cash-intensive businesses and "gatekeepers" acting on behalf of clients.

Product and Service Risk Analysis

Primeon Payments Limited evaluates potential risks associated with offered products and services, including innovative offerings or internationally border-crossing services. Risk factors consider services deemed high-risk by authorities and activities allowing anonymity or cross-border transactions.

2. Risk Mitigation Strategies at Primeon Payments Limited

- Customer Identification, Due Diligence, and Know Your Customer: Primeon Payments Limited has a Customer Identification Program (CIP) in place to ensure personnel can confidently identify each customer, understand their business activities, and assess associated risks. This program includes:
- Timely identification and verification of customer identity.
- Measures to identify beneficial owners.
- Gathering additional information to comprehend customer circumstances and expected transactions.
- Assessing customer risks based on various factors.

For higher-risk customers, enhanced due diligence is conducted, involving increased awareness, thorough documentation, account approval escalation, and ongoing monitoring.

- Monitoring of Customers and Transactions
  The monitoring approach at Primeon Payments Limited is tailored to the company's size, identified AML risks, and monitoring methods used. Monitoring is conducted based on perceived risks linked to customer behavior, products/services used, and transaction locations. The

Company's risk-based monitoring system responds to enterprise-wide issues, establishing thresholds for activity review and regularly reassessing system adequacy.

3. Suspicious Transaction Reporting

Primeon Payments Limited complies with regulatory requirements to report suspicious transactions, aiding authorities in combating financial crimes. A risk-based approach is utilized to identify suspicious activities, directing resources towards higher-risk areas. The Company enhances its suspicious activity identification approach with information from state and federal authorities and ensures periodic assessment of employee training and assessment adequacy.

4. Training and Awareness

The Company provides AML Program training tailored to staff roles, detailing AML laws, regulations, and internal policies. Training is provided at appropriate levels of detail, frequency, and tested for knowledge retention.

Non-acceptable Customers at Primeon Payments Limited

The Company refrains from engaging with clients involved in prohibited activities such as drug trade, arms dealing, or illegal services. Primeon Payments Limited prohibits anonymous accounts, shell banks, and maintaining relationships with individuals or entities associated with criminal or terrorist activities.

SUSPICIOUS TRANSACTIONS REPORTING PROCEDURES AT PRIMEON PAYMENTS LIMITED

Identification of Suspicious Activities:

- Primeon Payments Limited highlights several behaviors indicating suspicious transactions, such as transactions lacking business rationale, excessive concern for secrecy, or reluctance to disclose legitimate fund sources.
- Customers showing unusual behavior, distributing funds among multiple accounts, engaging in significant inter-account transfers, or conducting disproportionate transactions may raise suspicion.

- Further, specific ML/TF indicators related to Money Services Businesses (MSBs) include requests for foreign exchange rates exceeding standard rates, unusual currency exchanges, or large money orders.

Suspect Transaction Reporting Process:

- In case employees identify suspicious activities, they are required to notify the Nominated Officer at Primeon Payments Limited responsible for issuing a Suspicious Transaction Report via the FINTRAC online system and informing senior management promptly.
- Emphasizing a team approach in anti-money laundering (AML) procedures, the Nominated Officer collaborates with the Compliance Team to address complex money laundering issues effectively.
- Staff members who identify suspicious customer behavior must report their suspicions promptly to the Nominated Officer using the internal 'Suspicious Transaction Report Form' containing essential details like transaction parties, funds' owner, verification process, transaction description, reason for suspicion, supporting evidence, and assets subject to international sanctions.
- Prompt reporting of suspicions is critical, complying with legal requirements either before or immediately after the suspicious transaction occurrence.

Safeguards and Resolutions:

- Staff at Primeon Payments Limited should seek consent from FINTRAC before proceeding with suspicious transactions, ensuring compliance without tipping off the customer.
- Upon receiving the internal STR from staff, the Nominated Officer decides whether to report to FINTRAC or law enforcement agencies or document reasons for not reporting.
- A comprehensive approach ensures that staff members who report suspicions fulfill their duties and receive legal protection, underscoring the importance of timely reporting for effective AML procedures.

Primeon Payments Limited adheres to stringent reporting processes for identifying and addressing suspicious transactions, ensuring compliance with regulations and proactive risk management practices.

AML TRAINING AND AWARENESS AT PRIMEON PAYMENTS LIMITED

Primeon Payments Limited conducts annual AML training for all employees, focusing on key aspects to:

- Understand relevant money laundering legislation, including Federal AML laws.
- Comprehend company policies, procedures, and controls regarding money laundering, along with any updates.
- Identify and address transactions possibly linked to money laundering.
- Recognize suspicious activities within their business contexts and the process for notifying the Nominated Officer.
- Familiarize with money laundering techniques, methods, and trends relevant to the company's operations.
- Understand employee roles in combating money laundering, including the Nominated Officer's identity and responsibilities.
- Stay informed on industry findings, recommendations, directives, and relevant information.

The AML training at Primeon Payments Limited is tailored to the company's specific activities, products, services, customers, distribution channels, business partners, transaction levels, and complexities. It covers various levels of money laundering risks and vulnerabilities associated with the company's operations.

ONGOING MONITORING PROCEDURES AT PRIMEON PAYMENTS LIMITED

Continual monitoring is a crucial aspect of effective AML/CTF systems, allowing a thorough understanding of customer activities and ensuring compliance with regulations.

Primeon Payments Limited's ongoing monitoring practices encompass:

- Regular review of customer-related documents, data, and information to verify their relevance and accuracy.
- Monitoring customer activities to ensure alignment with their business nature, risk profile, and fund sources. Unusual transactions that

deviate from the expected patterns or lack apparent economic purpose are flagged for review.

In determining the best monitoring approach, Primeon Payments Limited considers:

- Business size and complexity.
- Assessment of ML/TF risks.
- Existing system controls and monitoring procedures.
- Product/service nature and delivery methods.

For identified complex or suspicious transactions, detailed examinations are conducted, documenting background information, transaction purpose, and outcomes for regulatory and audit purposes.

Risk-Based Monitoring Approach:

The level of monitoring at Primeon Payments Limited is tailored to the customer's risk profile determined through risk assessment procedures. Higher-risk relationships, including those involving Politically Exposed Persons (PEPs), undergo more stringent and frequent monitoring.

On a risk-based approach, ongoing monitoring considers factors like transaction nature, volume, geographical locations, and normal customer behavior. Changes in the relationship over time, such as new products/services, altered structures, or increased transactions, trigger enhanced monitoring and further Customer Due Diligence (CDD) procedures.

Primeon Payments Limited follows a systematic approach to identifying suspicious activities, comprising four key steps:

1. Screening

As a first step, screening involves recognizing indicators of suspicious activity commonly linked to money laundering. These include:

- Large or frequent cash transactions, either deposits or withdrawals.
- Patterns of suspicious activity like using accounts as temporary fund repositories or engaging in structured transactions.

- Involvement of entities commonly associated with money laundering, such as shelf companies or casinos.
- Currencies, countries, or nationals known for international crime or drug trafficking.
- Refusal to provide a legitimate explanation of financial activities.
- Activity that deviates from the expected norm based on the customer's history.
- Engagement with countries or nationals associated with terrorist activities.
- Transactions involving International and Politically Exposed Persons (PEPs).

2. Asking

When transactions show suspicious indicators, Primeon Payments Limited engages customers to explain the transaction's purpose, the source of funds, and the ultimate beneficiary. Assessing the customer's explanation for reasonableness determines whether the activity is deemed suspicious, leading to the potential submission of a suspicious transaction report.

3. Finding Out:

Tailored questions are posed to customers to understand the reasons behind transactions exhibiting suspicious activity indicators. For instance, probing further when observing structured remittances received. Legitimate businesses typically provide clear answers, while individuals involved in illicit activities may be evasive, providing partial or inaccurate explanations.

4. Evaluating:

The final step involves a decision on whether to submit a suspicious transaction report. While there are no exact guidelines due to the subjective nature of suspicion, a thorough evaluation of all circumstances ensures a high-quality decision-making process. If after thorough consideration Primeon Payments Limited deems the activity genuinely suspicious, an STR is recommended.

Primeon Payments Limited prioritizes meticulous ongoing monitoring practices, utilizing a risk-based approach to identify and address suspicious activities effectively, fostering a robust AML compliance framework.

RECORD-KEEPING PRACTICES AT PRIMEON PAYMENTS LIMITED

Primeon Payments Limited retains all business transaction records for a minimum of five years post the conclusion of the business relationship.

The purpose of record-keeping is to facilitate law enforcement in reconstructing business transactions long after their completion, ensuring a clear audit trail.

Required records include:

- Evidence of customer identity obtained as part of customer due diligence requirements;
- Supporting records for business relationships or occasional transactions subject to customer due diligence or ongoing monitoring;
- Documentation detailing the first client identification and verification processes;
- Any documents justifying exemptions from identification.

Specifically, regarding customer identity evidence, businesses must keep records of:

- Accepted identification documents and verification evidence copies;
- References to customer identity evidence.

Transaction and business relationship records like account files, correspondence, logbooks, receipts, and cheques should be maintained in a format enabling a comprehensive audit trail and the establishment of a financial profile for any suspicious account or customer.