ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING (AML/CFT) POLICY

Document Version: 1.0
Effective Date: 12 October 2026
Policy Owner: Management
Approved By: The Board of Directors
Review Frequency: At least annually and whenever material changes occur

---

1. PURPOSE

Metaramp Technologies Limited (“Metaramp” or “the Company”) is committed to preventing its business activities, technology services and business relationships from being used for money laundering, terrorist financing, proliferation financing, sanctions evasion, fraud or other financial crimes.

This Anti-Money Laundering and Counter-Terrorist Financing Policy (“AML/CFT Policy” or “the Policy”) establishes the principles and procedures through which the Company will identify, assess, mitigate and escalate financial crime risks associated with its activities.

The objectives of this Policy are to:

- Establish a risk-based framework for identifying and managing money laundering and terrorist financing risks.
- Promote appropriate customer identification and verification.
- Establish requirements for identifying ultimate beneficial owners and persons exercising control.
- Address sanctions screening, Politically Exposed Persons (PEPs), adverse media and other financial crime risks.
- Establish expectations for enhanced due diligence, suspicious activity escalation and recordkeeping.
- Define the Company's approach to third-party service provider oversight.

- Support compliance with applicable laws, regulations and contractual obligations.
- Protect the Company, its customers and its business partners from financial crime, legal and reputational risks.

The Company will implement this Policy in a manner proportionate to its business model, operational stage, risk exposure and applicable legal obligations.

2. SCOPE AND APPLICATION

This Policy applies to the Company's directors, management, employees, contractors and other representatives acting on its behalf.

It also establishes the principles that guide the Company's relationships with technology providers, payment service providers, financial institutions and other third parties involved in delivering its services.

The Policy covers financial crime risks associated with:

- Business onboarding and customer relationships.
- Customer identification and verification.
- Ultimate beneficial ownership and control.
- Sanctions, PEP and adverse media screening.
- Enhanced due diligence and source-of-funds assessments.
- Cross-border business payments and supported currencies.
- Stablecoin-related payment activity, where applicable.
- Transaction monitoring and suspicious activity escalation.
- Prohibited and restricted industries.
- Recordkeeping, confidentiality and information security.
- Third-party compliance arrangements and regulatory cooperation.

All relevant personnel must comply with this Policy and escalate suspected breaches or financial crime concerns through the appropriate channels.

This Policy must be read alongside applicable laws, contractual agreements, service-provider requirements and any additional compliance procedures adopted by the Company.

Nothing in this Policy overrides a legal or regulatory obligation that applies directly to Metaramp.

3. BUSINESS MODEL AND OPERATING STRUCTURE

Metaramp is a technology company providing software-enabled services to individuals and businesses. Its intended commercial model includes business-to-business services and access to cross-border business payment capabilities through third-party technology and financial service infrastructure.

The intended customer base includes businesses incorporated in Nigeria, the United States, Canada and other supported jurisdictions, subject to applicable eligibility requirements and restrictions.

The intended offering may support payments involving USD, GBP, EUR and supported stablecoins, depending on the capabilities and permitted use of the relevant service providers. Domestic Nigerian naira payment services are not part of the Company's current intended offering.

Under its intended operating model:

1. Customers discover or access the service through Metaramp's website, brand or other authorised digital entry point.
2. Customers complete the applicable onboarding and verification process through the designated service channels.
3. Account provision, payment processing, customer funds handling and movement of funds are performed by the parties responsible for those functions under the relevant arrangements.
4. Metaramp provides its technology-enabled services and customer entry point and does not intend to independently hold customer funds, operate payment infrastructure or execute payment transactions outside its established third-party arrangements.

The allocation of responsibility for customer due diligence, sanctions screening, transaction monitoring, suspicious activity reporting, record retention and regulatory engagement will depend on applicable law and the contractual arrangements among the parties.

The Company will seek to document these responsibilities and will not represent that a control is performed by Metaramp or a third party unless that representation is accurate.

This description reflects the Company's intended operating model and does not imply that the services are already operational or that any financial services licence or regulatory approval has been obtained.

4. GOVERNANCE AND RESPONSIBILITIES

4.1 Risk and Compliance Function

The Risk and Compliance Function shall coordinate the implementation of this Policy and support the identification, assessment, monitoring, and escalation of money laundering, terrorist financing, sanctions, and other financial crime risks relevant to the Company's activities.

Its responsibilities shall include:

- Maintaining and periodically reviewing the Company's AML/CFT risk assessment and related procedures.

- Coordinating customer due diligence, beneficial ownership verification, sanctions screening, politically exposed person (PEP) screening, and adverse media checks, as applicable to the Company's role and operating arrangements.
- Reviewing and escalating identified risk indicators, unusual activity, and potential policy breaches.
- Coordinating with relevant third-party service providers on compliance matters within the scope of their contractual responsibilities.
- Maintaining appropriate records of compliance decisions, escalations, incidents, and corrective actions.
- Monitoring relevant changes in applicable laws, regulations, and financial crime risks.
- Recommending updates to this Policy and related controls where necessary.

The Risk and Compliance Function refers to the personnel or appropriately qualified external professional designated by the Company to coordinate its AML/CFT responsibilities. Depending on the Company's operational structure and applicable requirements, these responsibilities may be performed internally or externally. The allocation of responsibilities shall be documented internally.

4.2 Personnel and Representatives

All personnel and representatives acting on behalf of the Company shall comply with this Policy, provide accurate information, maintain appropriate confidentiality, and promptly report suspected financial crime or compliance concerns through the designated reporting channel.

4.3 Third-Party Service Providers

Where third-party service providers perform customer onboarding, identity verification, sanctions screening, transaction monitoring, payment processing, or other compliance functions, their responsibilities shall be determined by applicable law and the relevant contractual arrangements.

The Company shall seek to understand the allocation of these responsibilities, maintain appropriate oversight proportionate to its role, and escalate relevant concerns through the appropriate channels.

4.4 Policy Approval and Oversight

The Board of Directors shall be responsible for approving this Policy and any material amendments, and for providing appropriate oversight of the Company's approach to managing money laundering, terrorist financing, sanctions, and other financial crime risks.

The Risk and Compliance Function shall coordinate the implementation and periodic review of this Policy, assess the need for amendments, and submit recommendations to the Board of Directors for consideration and approval.

The Board of Directors may delegate specific responsibilities in accordance with the Company's governance arrangements and applicable legal requirements. Any such delegation shall be documented internally.

The existence of the Risk and Compliance Function does not, by itself, represent that the Company holds a regulatory licence or that any regulated activity has been authorised.

5. RISK-BASED APPROACH

Metaramp will apply a risk-based approach to identify, assess and mitigate financial crime risks associated with its business model, customers, jurisdictions, products and third-party relationships.

The level of due diligence and oversight should be proportionate to the nature and severity of the identified risks.

5.1 Risk Factors

Relevant risk factors include:

- The customer's country of incorporation, operating locations and principal place of business.
- The customer's industry, business model and stated purpose for using the service.
- The identity, ownership and control structure of the business.
- Exposure to sanctions, PEPs, adverse media or high-risk jurisdictions.
- The legitimacy and commercial rationale of expected transactions.
- Transaction size, frequency, counterparties and payment corridors.
- The use of stablecoins or other digital-asset-related payment arrangements.
- Unusual changes in customer activity, ownership or transaction patterns.
- The adequacy of controls operated by relevant third-party providers.
- Applicable legal, regulatory and contractual restrictions.

5.2 Risk Classification

Where required by the applicable onboarding or compliance process, customers and business relationships should be classified according to their risk profile, such as low, medium or high risk.

The assessment should consider the relevant risk factors collectively rather than relying on a single indicator.

5.3 Risk Mitigation

Depending on the identified risk, appropriate measures may include:

- Standard customer due diligence.
- Enhanced due diligence.
- Additional documentation or verification.
- Further investigation of sanctions, PEP or adverse media matches.
- Additional review of source of funds or source of wealth.
- Senior-level approval where required.
- Increased monitoring or transaction restrictions.
- Declining or terminating a relationship where risks cannot be adequately mitigated.

5.4 Review of Risk Assessments

Risk assessments should be revisited when there is a material change in a customer's ownership, business activities, jurisdictions, transaction behaviour, service-provider arrangements or applicable legal requirements.

The Company will also review its overall financial crime risk exposure when its products, customer base or operating model materially change.

6. CUSTOMER DUE DILIGENCE AND VERIFICATION

Metaramp is committed to ensuring that business relationships are established with legitimate customers whose identities, ownership structures and intended activities can be reasonably understood.

Customer due diligence (CDD) must be conducted by the party responsible for onboarding under the applicable legal and contractual arrangements. Metaramp will provide accurate information about its own business and cooperate with reasonable verification requirements.

6.1 Business Identification and Verification

Depending on the customer's jurisdiction, legal structure and risk profile, the onboarding process may require:

- Certificate of incorporation or equivalent business registration documents.
- Business registration number and registered address.
- Information about the nature, purpose and principal activities of the business.
- Details of directors, authorised representatives and persons exercising control.
- Valid identification documents for relevant individuals.
- Evidence of business address, where required.
- Information on expected account usage, transaction volumes and payment corridors.
- Relevant licences or regulatory approvals for businesses conducting regulated activities.

6.2 Ultimate Beneficial Ownership

The ultimate beneficial owners (UBOs) of a business must be identified and verified in accordance with applicable requirements.

The process should establish the natural persons who ultimately own or control the customer, whether through direct or indirect ownership, voting rights or other means of control.

Where ownership structures are complex or involve multiple corporate entities, additional documentation may be required to establish the ownership chain and identify the individuals exercising ultimate control.

Where the beneficial ownership structure cannot be reasonably established, the relationship should be escalated for further review and should not proceed where applicable requirements cannot be satisfied.

6.3 Verification of Business Purpose

The customer's stated business activities and intended use of the service should be consistent with the information and documents provided.

Additional information may be requested where the business purpose is unclear, the expected transactions appear inconsistent with the customer's activities, or there are concerns about the legitimacy of the business relationship.

6.4 Incomplete or Inconsistent Information

Material inconsistencies, suspected forged documents or deliberately misleading information must be escalated for review.

Where required verification remains incomplete, the responsible party should defer, restrict or decline the relationship in accordance with applicable law and the relevant service arrangements.

6.5 Ongoing Customer Due Diligence

Customer information should be reviewed and updated when required by the customer's risk classification, applicable legal requirements or material changes in the relationship.

Relevant triggers may include changes in ownership, directors, business activities, operating jurisdictions or expected transaction patterns.

7. SANCTIONS, POLITICALLY EXPOSED PERSONS AND ADVERSE MEDIA SCREENING

Screening is a core component of the Company's financial crime risk framework. The responsible party must conduct screening appropriate to the relationship, relevant jurisdictions, applicable law and contractual arrangements.

7.1 Sanctions Screening

Relevant customers, ultimate beneficial owners, directors, authorised representatives and other parties requiring screening should be checked against applicable sanctions lists.

Depending on the jurisdictions and services involved, relevant sources may include:

- United Nations Security Council sanctions lists.
- Applicable Nigerian sanctions designations and restrictions.
- United States sanctions lists, including relevant Office of Foreign Assets Control (OFAC) lists, where applicable.
- United Kingdom sanctions lists, where applicable.
- Other national or international sanctions lists required by applicable law or the relevant service arrangement.

Screening must be proportionate to the risks and legal requirements applicable to the relationship.

Potential matches must be investigated before a relationship or transaction proceeds where required. Confirmed matches and unresolved material concerns must be escalated to the responsible compliance function.

The Company must not knowingly facilitate transactions prohibited by applicable sanctions or restrictions.

7.2 Politically Exposed Persons (PEPs)

Relevant customers and associated individuals should be screened to identify domestic or foreign Politically Exposed Persons, as well as relevant family members and known close associates, in accordance with applicable requirements.

A PEP identification does not automatically require rejection. However, where required by law or justified by the risk assessment, enhanced due diligence must be applied.

Measures may include:

- Establishing the source of funds and, where appropriate, source of wealth.
- Understanding the purpose and expected nature of the business relationship.

- Obtaining senior-level approval where required.
- Applying enhanced ongoing monitoring.
- Documenting the risk assessment and decision.

7.3 Adverse Media Screening

Relevant customers, beneficial owners, directors and associated individuals should be screened against credible media sources and other reliable information sources for adverse information relevant to financial crime and integrity risks.

Relevant concerns may include:

- Money laundering or terrorist financing.
- Fraud, embezzlement or financial misconduct.
- Corruption, bribery or abuse of public office.
- Sanctions evasion or proliferation financing.
- Organised crime or other serious criminal conduct.
- Material regulatory enforcement actions relevant to the proposed relationship.

Adverse information must be assessed for credibility, relevance, recency and its connection to the individual or business concerned. Unverified allegations must not automatically be treated as proof of wrongdoing.

Material concerns must be documented and escalated for a risk-based decision.

7.4 Potential Matches and False Positives

Potential sanctions or screening matches must be reviewed by the responsible party before a decision is made.

Where a potential match is determined to be a false positive, the basis for that determination should be documented in accordance with the applicable recordkeeping arrangements.

Where a match cannot be resolved satisfactorily, the relationship or transaction should be escalated and restricted where required by law or the applicable service arrangement.

7.5 Ongoing Screening

Screening should not be treated solely as a one-time onboarding exercise. Relevant parties should be re-screened periodically and when material events occur, including changes in ownership, risk classification, sanctions status or other relevant circumstances.

The frequency and scope of re-screening should be proportionate to risk and consistent with applicable legal requirements and the relevant service arrangement.

8. ENHANCED DUE DILIGENCE

Enhanced due diligence (EDD) must be applied where required by law or where a customer, transaction, jurisdiction or business relationship presents elevated financial crime risk.

8.1 Circumstances Requiring Enhanced Review

Triggers may include:

- PEP exposure.
- Material adverse media.
- Complex or opaque ownership structures.
- Exposure to high-risk jurisdictions or payment corridors.
- Unusually large or complex transactions inconsistent with the stated business.
- Unclear commercial rationale for a payment.
- Unexplained third-party payments or intermediaries.
- Suspected fraud, sanctions evasion or other financial crime.
- Elevated risks associated with stablecoins or digital-asset-related activity.
- Other circumstances identified through the Company's risk assessment or applicable requirements.

8.2 Enhanced Due Diligence Measures

Depending on the circumstances, EDD may include:

- Additional verification of the customer, beneficial owners and authorised representatives.
- Further information about business activities and counterparties.
- Evidence of source of funds or source of wealth.
- Supporting invoices, contracts, purchase orders or trade documents.
- Additional review of the intended payment purpose and expected activity.
- Verification of relevant business licences or regulatory approvals.
- Senior-level approval where required.
- Increased monitoring or transaction restrictions.

8.3 Source of Funds and Source of Wealth

Where warranted, the responsible party should obtain sufficient information to understand the origin of funds intended for a transaction and, where relevant, the broader source of a customer's wealth.

The evidence required will depend on the customer's risk profile, the nature and value of the transaction, and applicable requirements.

Potential supporting documents may include business contracts, invoices, financial statements, bank statements, tax documents or other reliable evidence.

8.4 Decisions Following Enhanced Review

Where EDD identifies concerns that cannot be adequately mitigated, the responsible party should decline, restrict, suspend or terminate the relationship or transaction as permitted or required by applicable law.

Material decisions should be documented, including the reasons for proceeding, applying restrictions or declining the relationship.

8.5 Allocation of Responsibility

Where a third-party provider is responsible for customer onboarding or enhanced due diligence, the relevant responsibilities should be established through the applicable contractual arrangements.

Metaramp will provide accurate information and escalate material concerns it identifies. The Company will not claim to have independently performed EDD unless it has actually done so.

9. SOURCE OF FUNDS AND COMMERCIAL PURPOSE

Metaramp recognises the importance of understanding the legitimate commercial purpose of business relationships and transactions.

Where required by the customer's risk profile, applicable law or the relevant service arrangement, the responsible party should assess whether the source of funds and stated transaction purpose are consistent with the customer's known business activities.

9.1 Supporting Information

Depending on the circumstances, customers may be asked to provide:

- Invoices or purchase orders.
- Supplier or customer contracts.
- Service agreements.
- Financial statements or relevant bank records.
- Business registration and licensing documents.
- Evidence of the origin of funds.
- Other documents reasonably necessary to establish the legitimacy of a transaction.

9.2 Indicators Requiring Further Review

Further review may be warranted where:

- A transaction lacks a credible commercial rationale.
- The payment is inconsistent with the customer's stated business.

- The source of funds cannot be reasonably explained.
- Funds are received from or sent to unrelated third parties without a clear business purpose.
- Transaction values or frequencies differ materially from the expected profile.
- Supporting documents appear inconsistent, altered or potentially fraudulent.
- The customer refuses to provide material information required for verification.

These indicators do not automatically establish criminal conduct but must be considered as part of a risk-based assessment.

9.3 Escalation and Restrictions

Material concerns must be escalated to the responsible compliance contact for further assessment.

Where appropriate, the responsible party may request additional evidence, apply restrictions, delay processing where legally permitted, or decline the transaction or relationship.

9.4 Metaramp's Own Corporate Information

Metaramp will provide accurate information about its own corporate activities, operating model and commercial arrangements when reasonably required for onboarding or compliance reviews.

The Company will not fabricate revenue, customer activity, funding sources, transaction history or supporting documents to satisfy onboarding requirements.

10. TRANSACTION MONITORING AND UNUSUAL ACTIVITY

Transaction monitoring is an important control for identifying activity that may be inconsistent with a customer's known business, expected transaction profile or legitimate commercial purpose.

10.1 Monitoring Responsibilities

Where transaction monitoring is performed by a third-party payment service provider or financial institution, the applicable responsibilities should be established through the relevant contractual arrangements.

The party responsible for monitoring should maintain controls proportionate to its legal obligations, services, customer risks and transaction exposure.

Metaramp will not represent that it independently operates transaction-monitoring systems unless such systems are actually implemented by the Company.

10.2 Indicators of Unusual Activity

Depending on the services and risks involved, monitoring controls should be designed to identify patterns such as:

- Transactions inconsistent with a customer's stated business or expected activity.
- Rapid movement of funds through accounts without a clear commercial rationale.
- Unexplained payments involving unrelated third parties.
- Unusual transaction splitting or structuring that may be intended to avoid controls.
- Unexpected activity involving high-risk jurisdictions.
- Suspected sanctions evasion or attempts to conceal counterparties.
- Patterns potentially associated with fraud, money laundering or terrorist financing.
- Unusual activity involving supported stablecoins or related service providers.
- Repeated failed or inconsistent verification attempts.
- Material discrepancies between transaction information and supporting documentation.

10.3 Escalation of Unusual Activity

Metaramp personnel must promptly escalate material concerns identified through customer interactions, business communications, operational information or other sources available to them.

The escalation should include, where available:

- The identity of the customer and relevant parties.
- A description of the activity or concern.
- Relevant dates, amounts, currencies and transaction references.
- Supporting communications or documents.
- The reasons the activity appears unusual or suspicious.

The responsible compliance contact should assess the concern and determine the appropriate next steps, including further investigation, restrictions, refusal or suspension of activity, and reporting to a competent authority where legally required.

10.4 Suspicious Activity and Confidentiality

Concerns must be handled promptly and confidentially. Personnel must not disclose the existence or status of a suspicious activity report or related investigation where such disclosure is prohibited by law.

Where a third-party provider is responsible for the relevant account or transaction, Metaramp will follow the agreed escalation process. This does not remove any reporting obligation that may independently apply to the Company.

10.5 Documentation

Material escalations and decisions should be documented in accordance with the Company's recordkeeping procedures and applicable legal requirements.

Records should capture the nature of the concern, information reviewed, actions taken, decisions made and relevant communications, subject to applicable confidentiality and data protection requirements.

11. PROHIBITED ACTIVITIES

Metaramp Technologies Limited will not knowingly support, facilitate or maintain business relationships involving activities that are unlawful, prohibited by applicable sanctions or inconsistent with the Company's financial crime risk standards.

Prohibited activities include:

1. Money laundering, terrorist financing or proliferation financing.
2. Transactions involving sanctioned persons, entities or jurisdictions where the relevant relationship or transaction is prohibited.
3. Fraud, scams, identity theft, forged documents or deliberate misrepresentation.
4. Concealment of criminal proceeds or transactions designed to disguise the origin, ownership or destination of funds.
5. Attempts to evade sanctions, customer verification, transaction monitoring or other applicable compliance controls.
6. Illegal trafficking in controlled substances, weapons, ammunition or explosives.
7. Human trafficking, forced labour, child exploitation or other serious criminal exploitation.
8. Unlawful gambling, betting or other prohibited commercial activities.
9. Unlicensed or unauthorised regulated financial services where the required authorisation is absent.
10. Other activities prohibited by applicable law or the relevant service provider's binding eligibility requirements.

The Company may decline, restrict, suspend or terminate a business relationship where credible concerns arise, subject to applicable law and contractual arrangements.

Where suspicious activity is identified, it must be escalated in accordance with Section 10 of this Policy.

12. PROHIBITED AND RESTRICTED INDUSTRIES

Metaramp recognises that certain industries present elevated financial crime, regulatory, legal or reputational risks. The Company will assess business activities and industry exposure during onboarding and, where appropriate, throughout the business relationship.

Customer eligibility remains subject to applicable law, required regulatory authorisations and the binding terms of the relevant service providers.

12.1 Prohibited Industries

Unless expressly permitted by applicable law and approved in writing by the relevant service providers, Metaramp will not knowingly onboard or facilitate transactions for businesses primarily engaged in:

- **Illegal activities:** Businesses selling illegal goods or services or conducting activities prohibited by applicable law.
- **Financial crime:** Businesses materially involved in money laundering, terrorist financing, sanctions evasion, fraud or the concealment of criminal proceeds.
- **Sanctioned activities:** Businesses or persons subject to restrictions that prohibit the proposed relationship or transaction.
- **Terrorism and prohibited proliferation financing:** Businesses supporting terrorist organisations or prohibited weapons proliferation.
- **Fraudulent schemes:** Businesses materially dependent on identity theft, forged documentation, deceptive investment schemes or deliberate misrepresentation.
- **Human exploitation:** Businesses involved in human trafficking, forced labour, child exploitation or other serious criminal abuses.
- **Illegal controlled substances:** Businesses trafficking in illegal narcotics or other prohibited controlled substances.
- **Unlawful weapons and restricted goods:** Businesses unlawfully manufacturing, selling or trafficking weapons, ammunition, explosives or other prohibited goods.
- **Unlawful gambling:** Gambling or betting businesses operating illegally or without required authorisations.

12.2 Restricted Industries

The following industries may be subject to enhanced due diligence, additional documentation, jurisdictional restrictions or prior written approval from the relevant service providers:

- **Gambling and betting:** Licensed casinos, sportsbooks, online gambling platforms and other wagering businesses.
- **Adult entertainment:** Businesses involved in adult content or related services, where permitted by law and by the relevant service providers.
- **Cannabis and related products:** Businesses operating in cannabis or cannabinoid markets, particularly where activities are treated differently across jurisdictions.
- **Arms, defence and dual-use goods:** Businesses dealing in regulated defence equipment, military goods or dual-use products.
- **Precious metals, stones and high-value goods:** Businesses dealing in gold, precious stones, luxury goods or other products associated with elevated money laundering risks.
- **Charities and non-profit organisations:** Where the nature, geography, ownership or transaction patterns create elevated terrorist-financing or other financial crime risks.

- **High-risk jurisdictions and complex cross-border structures:** Businesses operating in, or transacting with counterparties in, jurisdictions subject to relevant sanctions, heightened financial crime concerns or applicable restrictions.

A business operating in a restricted industry will not automatically be accepted or rejected solely because of its industry classification. The decision will depend on the nature of the business, its risk profile, required licences, applicable law and the policies of the relevant service providers.

12.3 Industry Screening and Approval

During onboarding and, where appropriate, ongoing monitoring, the responsible party should assess the customer's business activities, applicable licences, ownership structure, jurisdictions, counterparties and intended use of the service.

Where a business falls within a prohibited category, the application or transaction must be declined or restricted as appropriate.

Where a business falls within a restricted category, the relationship may proceed only after the required due diligence, regulatory checks and approvals have been completed.

Metaramp will not represent that a restricted industry has been approved by a service provider unless the relevant approval has been obtained.

The Company may update these categories in response to changes in applicable law, its risk assessment or the eligibility requirements of its service providers.

13. STABLECOIN AND DIGITAL-ASSET-RELATED RISKS

Where supported stablecoins or other digital-asset-related payment arrangements form part of the Company's services, the relevant parties must consider the additional risks associated with these activities.

13.1 Risk Assessment

Relevant risks may include:

- Transfers involving sanctioned persons or prohibited jurisdictions.
- Wallet addresses associated with suspected illicit activity.
- Exposure to fraud, scams, ransomware or other criminal proceeds.
- Obscured ownership or control of digital-asset wallets.
- Transactions involving unapproved exchanges, intermediaries or service providers.
- Unexplained transfers inconsistent with the customer's stated business.
- Use of unsupported assets, networks or transaction routes.

13.2 Appropriate Controls

Depending on the service arrangement, applicable law and the allocation of responsibilities, appropriate controls may include:

- Customer identification and verification.
- Sanctions screening of relevant parties.
- Review of wallet addresses and blockchain-related risk indicators where supported.
- Assessment of transaction purpose and counterparties.
- Additional documentation for higher-risk transactions.
- Escalation of suspected illicit activity.
- Restrictions on unsupported assets, wallets, jurisdictions or transaction types.

13.3 Responsibility and Escalation

Where blockchain analytics, wallet screening or digital-asset transaction monitoring is performed by a third-party provider, the relevant responsibilities should be established through the applicable arrangements.

Metaramp will escalate material concerns it identifies and will not claim to independently perform blockchain analytics or digital-asset monitoring unless those controls are actually implemented by the Company.

The Company will not knowingly facilitate digital-asset transactions prohibited by applicable law or binding service-provider restrictions.

14. THIRD-PARTY SERVICE PROVIDER OVERSIGHT

Metaramp's intended business model may depend on external technology platforms, payment service providers, financial institutions and other specialist providers.

The Company will seek to understand the allocation of responsibilities for the following functions, as applicable:

- Customer onboarding and identity verification.
- Ultimate beneficial ownership identification.
- Sanctions, PEP and adverse media screening.
- Ongoing customer due diligence.
- Enhanced due diligence.
- Transaction monitoring.
- Suspicious activity escalation and regulatory reporting.
- Payment execution and funds handling.
- Customer complaints and service restrictions.
- Compliance record retention and access.

- Cooperation with lawful regulatory or law-enforcement requests.

14.1 Due Diligence on Providers

Before entering into or materially changing a relevant arrangement, Metaramp should assess the provider's suitability in proportion to the services provided and the associated risks.

Where relevant and reasonably available, the assessment may consider:

- Corporate identity and reputation.
- Regulatory status and required authorisations.
- The scope of services provided.
- Security and data protection arrangements.
- Relevant compliance controls.
- Contractual allocation of responsibilities.
- Procedures for incident escalation and cooperation.

14.2 Documentation and Review

Relevant contracts, service descriptions, compliance communications and material decisions should be retained in accordance with the Company's recordkeeping arrangements.

Material changes to a provider's services, regulatory status or compliance arrangements should be reviewed for their potential impact on Metaramp's operations and risk exposure.

14.3 Limitations of Reliance

The use of a third-party provider does not automatically discharge obligations that apply directly to Metaramp under applicable law.

Where a control is essential to the Company's intended operating model, Metaramp should seek reasonable confirmation that an appropriate arrangement exists.

If a material control gap is identified, the Company should assess the risk and take appropriate action, which may include seeking remediation, restricting the affected activity or reconsidering the arrangement.

15. RECORDKEEPING

Metaramp will maintain appropriate records of its corporate activities, third-party arrangements, compliance decisions, material escalations, training and policy reviews.

15.1 Records to Be Maintained

Depending on the Company's activities and legal obligations, relevant records may include:

- Corporate registration and ownership documents.
- Third-party service agreements and compliance correspondence.
- AML/CFT risk assessments.
- Internal compliance escalations and decisions.
- Records of policy approval, review and amendment.
- Training and awareness records.
- Relevant customer or transaction information lawfully obtained by the Company.
- Records of incidents and corrective actions.

15.2 Retention Periods

Records must be retained for the period required by applicable law and relevant contractual obligations.

Where a specific retention period applies, the Company will follow that requirement. Records must not be destroyed where their retention is required for an ongoing investigation, lawful request or other legal obligation.

15.3 Third-Party Records

Where customer due diligence or transaction records are maintained by a third-party provider, access, retention and cooperation arrangements should be addressed in the applicable contract or service documentation.

Metaramp will retain records it is responsible for maintaining and cooperate with lawful requests within the scope of its obligations.

15.4 Security and Access

Records must be accurate, appropriately secured and accessible only to authorised persons with a legitimate business, legal or compliance need.

Personal and confidential information must be handled in accordance with applicable data protection requirements and the Company's information security practices.

16. TRAINING AND AWARENESS

Metaramp Technologies Limited shall promote awareness of money laundering, terrorist financing, sanctions evasion, fraud, and other financial crime risks relevant to its business activities.

The Company shall ensure that personnel involved in business development, customer relationships, operations, compliance coordination, and third-party service provider management understand their responsibilities under this Policy.

Training and awareness activities shall, as appropriate:

- Explain the Company's AML/CFT obligations and internal procedures.
- Identify common indicators of suspicious activity and financial crime.
- Explain the importance of accurate customer, beneficial ownership, and business information.
- Cover sanctions, politically exposed persons (PEPs), adverse media, and enhanced due diligence.
- Explain how concerns should be escalated and documented.
- Reinforce confidentiality and restrictions on disclosing suspicious activity reports or related investigations.

Training shall be provided during onboarding of relevant personnel and periodically thereafter, with additional guidance where material changes in the Company's business model, risk exposure, or applicable legal requirements make it necessary.

Where relevant AML/CFT functions are performed by third-party service providers, the Company shall seek to understand the providers' relevant controls and responsibilities and ensure that its own personnel understand the limits of the Company's role.

17. DATA PROTECTION AND CONFIDENTIALITY

Metaramp Technologies Limited shall handle personal data, business information, identity documents, beneficial ownership information, screening results, and other compliance records in accordance with applicable data protection and confidentiality requirements.

The Company shall seek to ensure that:

- Information is collected and used for legitimate business, verification, risk management, legal, or compliance purposes.
- Access to sensitive information is restricted to authorised persons who require it for their responsibilities.
- Information is transmitted and stored using appropriate security measures.
- Personal data is shared with third-party service providers only where there is an appropriate legal basis and the sharing is necessary for the relevant purpose.
- Information is retained only for the period required by applicable law, legitimate business needs, or relevant contractual obligations, and is securely disposed of when no longer required.
- Requests relating to personal data are handled in accordance with applicable data protection requirements.

Personnel must maintain the confidentiality of customer information, screening results, internal investigations, and compliance escalations. No person shall disclose information where doing so would breach applicable law, compromise an investigation, or constitute prohibited tipping-off.

18. BREACHES, INCIDENTS AND CORRECTIVE ACTION

Any suspected breach of this Policy, material weakness in an AML/CFT control, sanctions-related concern, suspicious activity, or failure by a relevant third-party service provider to perform an agreed compliance function shall be escalated promptly to the designated Risk and Compliance function.

Depending on the nature and seriousness of the matter, the Company may:

- Record and assess the incident.
- Request additional information or supporting documentation.
- Escalate the matter to the relevant third-party service provider or professional adviser.
- Suspend or discontinue a business relationship where appropriate and legally permissible.
- Take corrective action to address control weaknesses.
- Make or support any report or notification required by applicable law, subject to the respective legal responsibilities of the Company and relevant service providers.
- Document the decision, action taken, responsible person, and any outstanding remediation.

Incidents shall be handled confidentially and on a need-to-know basis. No employee or representative shall knowingly conceal a material compliance concern, falsify records, or obstruct an internal or external investigation.

19. LEGAL AND REGULATORY FRAMEWORK

This Policy shall be interpreted in line with applicable Nigerian law and any other legal or regulatory requirements relevant to the Company's activities, counterparties, jurisdictions, and operating arrangements.

Relevant legislation and frameworks may include, where applicable:

- The Money Laundering (Prevention and Prohibition) Act, 2022.
- The Terrorism (Prevention and Prohibition) Act, 2022.
- The Nigeria Data Protection Act, 2023.
- Applicable sanctions requirements and directives.
- Relevant regulations, guidance, and requirements issued by competent Nigerian authorities.
- Applicable foreign laws and regulatory requirements relevant to the Company's business relationships and cross-border activities.

The specific obligations applicable to the Company shall depend on its actual activities, legal status, contractual arrangements, and the roles performed by it and its third-party service providers.

This Policy does not, by itself, constitute a licence, regulatory approval, exemption, or authorisation to conduct any regulated activity. The Company shall not represent that it is authorised to perform a regulated financial service unless the required authorisation or other lawful basis has been established.

Where a legal or regulatory requirement conflicts with a provision of this Policy, the applicable legal requirement shall prevail. The Company shall seek appropriate professional advice where clarification is necessary.

20. POLICY REVIEW

This Policy shall be reviewed at least annually and whenever there is a material change in the Company's business model, customer base, geographical exposure, products, third-party service provider arrangements, applicable legal requirements, or identified financial crime risks.

Reviews shall consider, as appropriate:

- The continued suitability of the Company's risk assessment.
- Changes to customer due diligence and screening procedures.
- Emerging money laundering, terrorist financing, sanctions, fraud, and digital-asset risks.
- Material incidents, compliance concerns, or control weaknesses.
- Changes in the responsibilities of the Company and its third-party service providers.
- Updates to applicable legislation, regulatory guidance, and contractual requirements.

Material amendments shall be documented and submitted to the Risk and Compliance function or other duly authorised person for approval. Superseded versions shall be retained where required for governance, audit, or regulatory purposes.