

AML/CFT Policy

Last Updated: July 27, 2026

1. Introduction

This Anti-Money Laundering and Counter-Terrorist Financing Policy ("AML/CTF Policy") applies to **mirocard.com** (the "Company"), an online platform that facilitates users' access to virtual payment cards made available by independent third-party providers. The Company does not issue payment cards and does not provide payment services in its own name.

The Company is committed to maintaining the highest standards of integrity and preventing its platform and services from being used for money laundering, terrorist financing, fraud, sanctions evasion, or any other form of financial crime. To support this commitment, the Company has adopted this AML/CTF Policy, which establishes a comprehensive framework for identifying, assessing, monitoring, and mitigating financial crime risks associated with its business activities.

This AML/CTF Policy is based on a risk-based approach and is designed to ensure compliance with all applicable anti-money laundering, counter-terrorist financing, sanctions, and financial crime prevention laws and regulations, as well as internationally recognized standards, including, where applicable, the Recommendations of the Financial Action Task Force ("FATF").

The purpose of this Policy is to:

- establish effective controls to prevent the misuse of the Company's platform and services for illicit purposes;
- define the Company's AML/CTF governance, roles, and responsibilities;
- ensure that appropriate Customer Due Diligence ("CDD"), Enhanced Due Diligence ("EDD"), where applicable, and ongoing monitoring measures are implemented in accordance with the Company's risk-based approach;
- facilitate the timely identification, investigation, escalation, and reporting of suspicious activities where required by applicable law; and
- promote a culture of compliance and financial crime risk awareness throughout the Company.

This Policy applies to all directors, officers, employees, contractors, consultants, and any other individuals acting for or on behalf of the Company in connection with the operation, management, or support of the Company's platform and services.

2. Policy Scope

This Policy applies to all business activities carried out by the Company in connection with the operation of its online platform and the provision of services facilitating users' access to virtual payment card products made available by independent third-party providers.

This Policy applies to:

- all directors, officers, employees, contractors, consultants, and other individuals acting for or on behalf of the Company;
- all Customers using the Company's platform and related services;
- all products and services provided through the Company's platform;
- all relevant third-party relationships involved in the delivery of the Company's services, to the extent required by applicable law and contractual arrangements.

This Policy establishes the AML/CTF standards applicable throughout the customer relationship, including customer onboarding, customer identification and verification, sanctions and politically exposed person ("PEP") screening, customer risk assessment, transaction monitoring (where applicable), ongoing customer due diligence.

All directors, officers, employees, contractors, consultants, and other individuals acting on behalf of the Company are required to understand and comply with this Policy.

The Company applies a risk-based approach to AML/CTF compliance to ensure that the level of due diligence and internal controls is proportionate to the money laundering, terrorist financing, proliferation financing, sanctions, fraud, and other financial crime risks associated with its customers, products, services, delivery channels, third-party relationships, and geographic exposure.

3. Definitions

For the purposes of this AML/CTF Policy, the following terms shall have the meanings set out below:

"AML/CTF" (Anti-Money Laundering and Counter-Terrorist Financing) means the policies, procedures, and controls implemented by the Company to prevent, detect, and mitigate risks related to money laundering, terrorist financing, sanctions violations, fraud, and other financial crimes.

"Company" has the meaning given to that term in the Terms of Use.

"Customer" has the meaning given to that term in the Terms of Use.

"Customer Due Diligence (CDD)" means the process of identifying, verifying, and assessing Customers to establish and verify their identity, understand the nature and purpose of the business relationship, and assess the associated financial crime risks.

"Know Your Customer (KYC)" means the procedures implemented by the Company to collect, verify, maintain, and, where appropriate, update Customer information, including identity verification, sanctions and PEP screening, and customer risk assessment.

"Enhanced Due Diligence (EDD)" means additional verification, information gathering, and ongoing monitoring measures applied to Customers, transactions, or business relationships identified as presenting a higher level of financial crime risk.

"Risk-Based Approach (RBA)" means the approach under which the Company applies AML/CTF measures proportionate to the level of financial crime risk associated with its Customers, products, services, transactions, delivery channels, third-party relationships, and jurisdictions.

"Politically Exposed Person (PEP)" means an individual who is or has been entrusted with a prominent public function, as well as their immediate family members and close associates, as defined under applicable AML/CTF laws and regulations.

"Sanctions" means restrictive measures imposed by competent governmental or international authorities, including, where applicable, the United Nations Security Council (UNSC), the Office of Foreign Assets Control (OFAC), the European Union (EU), the United Kingdom Office of Financial Sanctions Implementation (OFSI), and any other applicable sanctions authorities.

"Restricted Jurisdiction" means any country, territory, or geographic region in respect of which the Company restricts or prohibits the provision of its services due to applicable sanctions, legal or regulatory requirements, financial crime risks, or internal risk management decisions.

"Transaction Monitoring" means the process of reviewing and analysing Customer activity and, where applicable, transactions associated with the Company's services in order to identify unusual, suspicious, or potentially unlawful activity.

"Suspicious Activity" means any activity, transaction, attempted transaction, or behaviour that gives rise to knowledge, suspicion, or reasonable grounds to suspect money laundering, terrorist financing, fraud, sanctions evasion, or any other financial crime.

"Financial Crime" means any actual or attempted unlawful activity involving financial or economic benefit, including, but not limited to, money laundering, terrorist financing, fraud, sanctions evasion, bribery, corruption, tax evasion, and other unlawful financial activities.

"Third-Party Service Provider" means any external entity engaged by or cooperating with the Company in connection with the provision of its services.

"Ongoing Due Diligence" means the continuous monitoring and periodic review of Customer relationships, including updating Customer information, reviewing Customer activity and, where applicable, transactions associated with the Company's services, and reassessing Customer risk throughout the business relationship.

4. Risk-Based AML/CTF Framework

The Company adopts a Risk-Based Approach ("RBA") to Anti-Money Laundering and Counter-Terrorist Financing ("AML/CTF") compliance, ensuring that its policies, procedures, and internal controls are proportionate to the level of financial crime risk associated with its business activities.

The Company's AML/CTF framework is designed to identify, assess, monitor, and mitigate the risks of money laundering, terrorist financing, fraud, sanctions evasion, and other financial crimes that may arise in connection with the Company's platform, services, Customers, and relationships with Third-Party Service Providers.

4.1 Risk Assessment

The Company performs ongoing assessments of its exposure to financial crime risks. Such assessments take into account, among other factors:

- the nature of the Company's products and services;
- risk characteristics;
- transaction size, frequency, and patterns, where applicable;
- delivery channels and methods of Customer interaction;
- geographic exposure and jurisdictional risks;
- payment methods and funding sources;
- Third-Party Service Providers involved in the delivery of the Company's services; and
- emerging financial crime threats, regulatory developments, and relevant typologies.

Risk assessments are reviewed periodically and whenever significant changes occur in the Company's business model, products, services, Customer base, Third-Party Service Providers, or the applicable legal and regulatory environment.

4.2 Customer Risk Classification

The Company assigns each Customer a risk rating based on its internal risk assessment methodology. Customers are generally classified as Low, Medium, or High Risk.

The Customer risk classification takes into account factors including:

- Customer identity and verification results;
- country of residence or location;
- sanctions, PEP, and adverse media screening results;
- expected use of the Company's services and anticipated activity;
- source of funds or source of wealth, where applicable;
- the involvement of higher-risk jurisdictions; and
- any other indicators of elevated financial crime risk.

Customer risk ratings are reviewed periodically and updated whenever new information or changes in Customer activity or risk indicators justify a reassessment.

4.3 Risk-Based Controls

The Company applies AML/CTF controls that are proportionate to the level of identified risk. Depending on the Customer's risk profile, the Company may apply:

- Standard Customer Due Diligence ("CDD") to lower-risk Customer relationships;
- Enhanced Due Diligence ("EDD") where higher financial crime risks are identified; and
- additional monitoring, verification, or approval measures where appropriate.

Higher-risk Customers, business relationships, or jurisdictions may be subject to enhanced scrutiny, additional verification requirements, more frequent reviews, and, where appropriate, approval by designated members of senior management.

4.4 Ongoing Risk Monitoring

Risk management is an ongoing process. The Company periodically reviews Customer relationships, updates Customer information, monitors Customer activity and, where applicable, transactions associated with the Company's services, and reassesses Customer risk throughout the business relationship.

4.5 Continuous Improvement

The Company periodically reviews and enhances its AML/CTF risk management framework to reflect changes in applicable laws and regulations, regulatory expectations, industry best practices, technological developments, and emerging financial crime risks. Policies, procedures, and internal controls are updated as necessary to ensure that the Company's AML/CTF programme remains effective, proportionate, and appropriate to its business activities and risk profile.

5. Customer Due Diligence (CDD)

The Company applies Customer Due Diligence ("CDD") measures as a fundamental component of its AML/CTF framework to ensure that Customers are appropriately identified, verified, and assessed before, or where permitted by applicable law, during the establishment of a business relationship.

CDD measures are designed to prevent the misuse of the Company's platform and services for money laundering, terrorist financing, fraud, sanctions evasion, or other financial crimes. The scope and extent of CDD measures are determined in accordance with the Company's Risk-Based Approach and the financial crime risk presented by each Customer.

5.1 Customer Identification and Verification

The Company collects and verifies Customer information using reliable, independent, and, where appropriate, electronic sources.

Depending on the level of identified risk and applicable legal or regulatory requirements, the Company may collect and verify:

- full name, date of birth, nationality, residential address, and other identifying information;
- government-issued identification documents;
- contact information and other relevant personal details;
- any additional information or documentation required to verify the Customer's identity.

The Company may use Third-Party Service Providers and technological solutions to assist with identity verification, document authentication, biometric verification, sanctions screening, and fraud prevention.

5.2 Customer Risk Assessment

Each Customer is subject to a risk assessment conducted in accordance with the Company's internal AML/CTF risk methodology.

The assessment may take into account, among other factors:

- Customer profile;

- country of residence or geographic exposure;
- expected use of the Company's services;
- anticipated activity and usage patterns;
- sanctions, PEP, and adverse media screening results;
- source of funds or source of wealth, where appropriate; and
- any other relevant financial crime risk indicators.

Based on the outcome of the assessment, Customers may be assigned different risk ratings, which determine the level of due diligence, monitoring, and internal controls applied.

5.3 Enhanced Due Diligence

Where higher financial crime risks are identified, the Company may apply Enhanced Due Diligence ("EDD") measures.

Depending on the circumstances, EDD measures may include:

- obtaining additional information or supporting documentation;
- verifying the source of funds or source of wealth, where appropriate;
- conducting enhanced review of Customer information or activity;
- increasing the frequency of ongoing monitoring;
- obtaining approval from designated compliance personnel or senior management before establishing or continuing the business relationship; and
- applying any other enhanced risk mitigation measures considered appropriate.

5.4 Ongoing Customer Monitoring

CDD is an ongoing process and continues throughout the duration of the Customer's business relationship with the Company.

The Company may perform ongoing monitoring by:

- monitoring Customer activity and, where applicable, transactions associated with the Company's services;
- periodically reviewing and updating Customer information;
- conducting sanctions, PEP, and adverse media re-screening;
- identifying and investigating unusual or suspicious activity; and
- conducting trigger-based reviews following material changes in the Customer's circumstances, activity, or risk profile.

Where the Company is unable to complete the required CDD measures, verify a Customer's identity, or adequately mitigate identified financial crime risks, the Company may decline to establish a business relationship or may restrict, suspend, or terminate the Customer's access to its services in accordance with applicable law, contractual arrangements, and the Company's internal policies.

6. Know Your Customer (KYC)

The Company maintains a Know Your Customer ("KYC") programme as a core component of its AML/CTF framework.

KYC measures are applied in accordance with the Company's Risk-Based Approach before, or where permitted by applicable law, during the establishment of a business relationship and

throughout its duration. The extent of KYC measures depends on the Customer's risk profile, the nature of the services used, geographic considerations, and other relevant financial crime risk factors.

6.1 KYC Identification Requirements

To establish and verify a Customer's identity, the Company may collect and verify information including:

- full legal name;
- date of birth;
- nationality;
- residential address;
- a valid government-issued identification document;
- email address and other contact information; and
- any additional information or documentation required to satisfy applicable legal, regulatory, or internal compliance requirements.

The Company may use reliable and independent sources, electronic verification systems, biometric verification technologies, and Third-Party Service Providers to assist in the identity verification process.

6.2 Screening and Risk Checks

As part of its KYC procedures, the Company performs screening designed to identify potential financial crime risks before establishing, and throughout, the Customer relationship.

Screening may include checks against:

- applicable sanctions lists;
- Politically Exposed Persons ("PEP") databases;
- adverse media sources;
- fraud prevention databases; and
- other internal or external compliance databases, where appropriate.

Where a potential match or elevated financial crime risk is identified, the Company may conduct additional reviews, request further information or documentation, apply Enhanced Due Diligence ("EDD"), or decline to establish or continue the Customer relationship, where appropriate.

6.3 KYC Information Updates

The Company takes reasonable measures to ensure that Customer information remains accurate, complete, and up to date throughout the business relationship.

Customers may be required to provide updated information or supporting documentation where:

- their personal information changes;
- unusual or potentially suspicious activity is identified;
- their risk profile changes;
- periodic KYC reviews are required based on the applicable risk level; or
- additional information is required to comply with legal or regulatory obligations.

Failure to provide requested information or documentation within a reasonable period may result in the restriction, suspension, or termination of the Customer's access to the Company's services, where permitted by applicable law.

6.4 KYC Records Management

KYC records are maintained in a secure manner, protected against unauthorized access, alteration, or disclosure, and retained only for the period required to comply with applicable legal, regulatory, contractual, and legitimate business obligations. Appropriate technical and organizational measures are implemented to safeguard the confidentiality, integrity, and availability of Customer information.

7. Sanctions Screening

The Company maintains a sanctions screening programme as an integral part of its AML/CTF framework to prevent its platform and services from being used by individuals or other persons subject to applicable sanctions, restrictive measures, or other legal prohibitions.

7.1 Screening requirements

The Company performs sanctions screening before establishing a business relationship with a Customer and periodically throughout the relationship in accordance with its Risk-Based Approach.

Screening may be conducted:

- during the Customer onboarding process;
- throughout the Customer relationship on a periodic or event-driven basis;
- following material changes to Customer information or risk profile; and
- following updates to applicable sanctions requirements.

The Company uses reliable screening systems and trusted data sources to identify potential matches against applicable sanctions lists.

7.2 Sanctions Lists and Data Sources

The Company conducts sanctions screening against applicable sanctions programmes issued by competent governmental and international authorities, including, where applicable:

- the United Nations Security Council (UNSC);
- the Office of Foreign Assets Control ("OFAC");
- the European Union (EU);
- the United Kingdom Office of Financial Sanctions Implementation (OFSI); and
- any other sanctions authorities relevant to the Company's operations.

7.3 Sanctions Compliance Monitoring

The Company maintains appropriate records of sanctions screening activities and periodically reviews and enhances its sanctions screening programme to reflect changes in applicable sanctions regimes, regulatory expectations, industry best practices, and emerging financial crime risks.

8. Transaction Monitoring and Suspicious Activity

The Company monitors Customer activity using a risk-based approach, taking into account, where applicable:

- transaction frequency, value, and patterns;
- Customer behaviour and expected use of the Company's services;
- activity involving higher-risk jurisdictions;
- attempts to circumvent applicable controls or restrictions; and
- indicators of fraud or other financial crime.

Monitoring may be supported by automated systems, manual reviews, and information provided by Third-Party Service Providers.

8.1 Review of Suspicious Activity

Where potentially suspicious activity is identified, the Company may:

- review available Customer information and activity;
- request additional information or documentation;
- apply Enhanced Due Diligence ("EDD");
- restrict, suspend, or terminate the Customer relationship, where appropriate; and
- take any other action required or permitted under applicable law.

8.2 Suspicious Activity Reporting

Where appropriate and as required or permitted by applicable law, the Company may report suspicious activity or cooperate with the relevant competent authorities, or Third-Party Service Providers responsible for regulatory reporting.

8.3 Ongoing Review

The Company periodically reviews and updates its transaction monitoring procedures to reflect changes in applicable laws, regulatory expectations, emerging financial crime risks, and the Company's business activities.

9. Record Keeping

The Company maintains records relating to its AML/CTF compliance programme, including, where applicable, Customer due diligence, risk assessments, monitoring activities, and compliance decisions. Records are retained for the period required by applicable law or the Company's legitimate business and compliance purposes.

The Company implements appropriate technical and organisational measures to protect AML/CTF records from unauthorised access, alteration, disclosure, or loss. Access to such records is limited

to authorised personnel and may be provided to competent authorities or relevant Third-Party Service Providers where required or permitted by applicable law.

10. Restricted Jurisdiction

The Company may restrict, limit, or prohibit access to its platform and services where a Customer's location, residence, activities, or other connection with a jurisdiction presents legal, regulatory, sanctions, fraud, or other financial crime risks.

10.1 Risk Assessment

In determining whether geographic restrictions apply, the Company may consider applicable laws, sanctions, regulatory requirements, information provided by competent authorities or Third-Party Service Providers, and its own internal risk assessment.

10.2 Restrictions

Where the Company determines that a Customer or jurisdiction presents an unacceptable legal, regulatory, or compliance risk, it may, at its sole discretion:

- refuse or discontinue onboarding;
- request additional information or documentation;
- restrict or suspend access to the Company's services; or
- terminate the Customer relationship.

10.3 Changes to Restrictions

The Company may establish, modify, or remove restrictions, including any list of restricted or unsupported jurisdictions, at any time without prior notice to reflect changes in applicable law, sanctions, regulatory or partner requirements, operational considerations, or the Company's internal risk assessment.

11. Policy Review and Updates

The Company may review and update this AML/CTF Policy from time to time to reflect changes in applicable law, regulatory expectations, its business activities, products or services, risk profile, or internal compliance requirements.

The Company reserves the right to amend this Policy at any time, with any updated version becoming effective upon publication or as otherwise determined by the Company.