Spend.Net — AML & CTF Policy

Effective date: 15 May 2026

---

1. Introduction

This Anti-Money Laundering and Counter-Terrorist Financing Policy (the "AML Policy") sets out the standards, controls, and procedures applied by Widberg Affiliates Limited, registered at Trust Company Complex, Ajeltake Road, Ajeltake Island, Majuro, Republic of the Marshall Islands, MH 96960 ("Spend.Net", "we", "us"), in operating the Spend.Net platform available at https://spend.net.

Spend.Net is a technology provider that delivers a virtual debit card program. Card issuance, the holding of customer funds, and underlying payment processing are performed by regulated issuing banks and payment service providers ("Issuing Partners"). Spend.Net is not a bank, money services business, electronic money institution, or other regulated financial institution and does not hold customer funds in its own name. We do not currently operate under a money services business or similar licence.

Notwithstanding the above, Spend.Net voluntarily applies a risk-based AML and counter-terrorist financing ("CTF") control framework that is aligned with the recommendations of the Financial Action Task Force (FATF) and with the AML/CTF requirements imposed on us by our Issuing Partners under contractual program-management arrangements. Where our Issuing Partners are subject to AML/CTF, sanctions, or financial-crime obligations under the laws applicable to them, the obligations relevant to the Spend.Net platform are contractually flowed down to Spend.Net, and Spend.Net acts in support of, and on behalf of, the Issuing Partner in performing those obligations. References in this AML Policy to the Acceptable Use and Restrictions Policy (the "AUP") are to the document previously titled "Internal Policy". This AML Policy explains how the framework is applied in practice.

2. Purpose and objectives

- Prevent the platform from being used as a vehicle for money laundering, terrorist financing, sanctions evasion, fraud, or other financial crime.
- Identify and verify our customers and, where relevant, their beneficial owners.
- Monitor customer activity on a risk-sensitive basis and detect unusual or suspicious patterns.
- Cooperate with our Issuing Partners, their regulators, and competent authorities in the prevention and detection of financial crime.
- Comply with applicable sanctions regimes and Issuing Partner requirements.

3. Scope

This AML Policy applies to all activities carried out by Spend.Net, including the onboarding of applicants, the issuance and use of virtual debit cards through our Issuing Partners, and all related customer activity. It is binding on:

- All employees, officers, and directors of the company;
- Contractors and consultants engaged by the company; and
- Third-party service providers acting on behalf of the company, including any sub-processors.

4. Governance and the Compliance Function

Overall responsibility for AML/CTF compliance rests with the board and senior management of Widberg Affiliates Limited. A named Compliance Officer / Money Laundering Reporting Officer (the "MLRO") is appointed internally, supported by a designated deputy to ensure coverage. The identity and contact details of the MLRO are recorded in our internal compliance records and disclosed to our Issuing Partners, their regulators, and competent authorities where required. The MLRO reports to senior management and to the board on a defined cadence (at least annually, and more frequently where matters require escalation), and maintains a documented decision log for internal escalations, suspicious-activity reviews, and material compliance decisions. The MLRO is responsible for:

- Maintaining and reviewing this AML Policy and supporting internal procedures.
- Acting as the central point of contact with Issuing Partners on AML/CTF matters.
- Reviewing escalations and internal suspicious-activity reports.
- Reporting suspicious activity to our Issuing Partners and, where applicable, to competent authorities.
- Coordinating staff training and periodic independent reviews of our controls.

5. Risk-based approach and customer risk assessment

Spend.Net operates a documented enterprise-wide risk assessment that considers customer, geographic, product, channel, and transaction risk factors. This risk assessment is reviewed at least annually and updated whenever there is a material change to our customer base, products, technology, or regulatory environment.

Each customer is assigned an AML risk rating (typically low, medium, or high) based on factors including, but not limited to:

- Customer type (individual, individual entrepreneur, or legal entity) and ownership structure.
- Country of residence or incorporation and any nexus to higher-risk jurisdictions.
- Source of funds and source of wealth (for higher-risk customers).
- Whether the customer or any beneficial owner is a Politically Exposed Person ("PEP").
- Expected and actual transaction patterns.

6. Customer onboarding, KYC and selfie verification

No virtual debit card is issued to a customer until that customer has completed Know-Your-Customer ("KYC") verification to our satisfaction. KYC is performed using a combination of in-house controls and specialised third-party identity-verification providers.

6.1 Individuals

For individual applicants, KYC includes as a minimum:

- Collection of full legal name, date of birth, nationality, residential address, contact details, and country of residence.
- Submission of a clear image of a valid government-issued photographic identity document (passport, national identity card, or residence permit) bearing a unique identification number.
- A live selfie / biometric liveness check, captured through our verification provider, and matched against the photograph on the identity document.
- Electronic verification of the data provided against independent and reliable sources where available.
- Screening against sanctions, PEP, and adverse-media databases.

6.2 Legal entities and individual entrepreneurs

For legal entities and individual entrepreneurs, KYC includes as a minimum:

- Certificate of incorporation or equivalent registration document, and (for entities older than 12 months) a certificate of good standing or equivalent.
- Articles of association, constitutional documents, and evidence of registered address.
- Identification of directors, authorised signatories, and beneficial owners (individuals who directly or indirectly own or control 10% or more of the entity), each verified using the individual KYC measures above, including a selfie / liveness check.
- Business description, expected activity, source of funds, and (where relevant) source of wealth.
- Screening of the entity and its directors, signatories, and beneficial owners against sanctions, PEP, and adverse-media databases.

6.3 Enhanced Due Diligence (EDD)

Enhanced Due Diligence is applied to higher-risk relationships, including PEPs and their close associates, customers with a nexus to higher-risk jurisdictions, and customers exhibiting unusual or higher-risk activity. EDD measures may include:

- Approval of the relationship at senior-management level.
- Verification of source of funds and source of wealth using documentary evidence.
- More frequent and granular ongoing monitoring.

- Additional information about the purpose and intended nature of the relationship.

6.4 Prohibited customers and refusal of service

We will not establish or maintain a relationship with any applicant or customer who:

- Refuses or fails to complete KYC, including the selfie / liveness check.
- Is the subject of applicable sanctions, or is owned or controlled by a sanctioned party.
- Is a citizen or resident of, is incorporated in, or is otherwise based in or acting from, any jurisdiction listed as restricted in our AUP, or is acting on behalf of any person connected to such a jurisdiction.
- Is reasonably suspected of involvement in money laundering, terrorist financing, fraud, or other financial crime.
- Provides false, misleading, or incomplete information.

7. Ongoing monitoring and transaction monitoring (KYT)

Customer relationships and transactions are subject to ongoing monitoring on a risk-sensitive basis. Our Know-Your-Transaction ("KYT") framework includes:

- Automated rules and scenarios designed to identify unusual or potentially suspicious patterns (for example, structuring, rapid in-and-out activity, atypical merchant categories, or transactions inconsistent with the customer profile).
- Real-time screening of card transactions against sanctions and high-risk merchant lists, in coordination with our Issuing Partners.
- Periodic review of customer profiles, with refreshed KYC documentation for higher-risk customers.
- Threshold-based escalation: transactions or aggregated activity exceeding defined thresholds are reviewed by the Compliance team.
- Investigation of alerts by trained analysts, with documented outcomes.

8. Sanctions compliance

Spend.Net screens applicants, customers, beneficial owners, related parties, and where appropriate counterparties against applicable sanctions lists, including those maintained by the United Nations Security Council, the Office of Foreign Assets Control of the United States, the European Union, His Majesty's Treasury (United Kingdom), and any other list required by our Issuing Partners. Sanctions screening is performed at onboarding, on an ongoing basis, and whenever lists are updated. Confirmed matches result in an immediate restriction of the relationship and, where required, reporting to the relevant authority.

9. Geographic restrictions

We do not provide services to applicants or customers who are citizens or residents of, who are incorporated in, or who are otherwise based in or acting from any of the jurisdictions listed as restricted in our AUP. Our virtual debit card solution also does not support merchants located in, or otherwise based in or acting from, certain jurisdictions, as set out in the AUP. The list of restricted customer jurisdictions in the AUP includes, among others, the Republic of the Marshall Islands. The lists of restricted jurisdictions may be updated from time to time to reflect changes to applicable sanctions, Issuing Partner and card scheme requirements, and our internal risk appetite, and are categorised in the AUP by reference to (i) sanctions or legal prohibition, (ii) Issuing Partner or card scheme restriction, and (iii) internal risk appetite, with the methodology and ownership of the list described in the AUP and supporting internal procedures.

10. Suspicious activity reporting

Where any employee, contractor, or system identifies activity that gives rise to reasonable grounds to suspect money laundering, terrorist financing, sanctions evasion, fraud, or other financial crime, an internal suspicious-activity report is raised and escalated to the Compliance Officer without delay.

The Compliance Officer evaluates internal reports and, where appropriate:

- Reports the matter to the relevant Issuing Partner, which may file a suspicious activity / transaction report with its competent financial intelligence unit;
- Reports the matter directly to a competent authority, where Spend.Net has an independent legal obligation to do so;
- Implements restrictions on the customer's Account, including suspension or termination, where appropriate; and
- Refrains from "tipping off" the customer about the existence or content of any such report, in line with applicable law.

11. Record-keeping

Spend.Net maintains records of customer identification, KYC evidence, compliance reviews, internal reports, escalations, and transactional information for a minimum of five (5) years from the end of the customer relationship or the date of the transaction, whichever is later, or for any longer period required by law or by our Issuing Partners. Records are stored securely, are retrievable, and may be shared with our Issuing Partners and with competent authorities, as required, subject to applicable law.

12. Employee training and awareness

All employees and relevant contractors receive AML/CTF training at induction and on an ongoing basis (at least annually). Training is tailored by role and covers, as a minimum, this AML Policy, sanctions, recognising and escalating suspicious activity, data-protection considerations, and the consequences of non-compliance. Completion of training is recorded.

13. Whistleblower protection

We encourage all employees, contractors, and partners to raise concerns about possible breaches of this AML Policy or of applicable law in good faith. Reports can be made confidentially to the MLRO by email at compliance@spend.net, which is monitored by the compliance function on a restricted-access basis. Reports are logged in a confidential whistleblowing register, are assessed by the MLRO (or, where the report concerns the MLRO, by senior management), and where appropriate are escalated to senior management, our Issuing Partners, or competent authorities. Spend.Net prohibits retaliation against any person who raises a concern in good faith, including dismissal, demotion, discrimination, or any other adverse treatment.

14. Independent review

The design and operating effectiveness of our AML/CTF controls are reviewed periodically, at least annually, by a function independent of day-to-day operations, and may also be reviewed by our Issuing Partners or by their regulators. Findings are reported to management and remediation actions are tracked through to closure.

15. Review and updates

This AML Policy is reviewed at least annually, and additionally whenever there is a significant change to our business, products, technology, customer base, or to the legal, regulatory, or contractual requirements applicable to us. The most recent version is always available on the Website.

16. Contact

Widberg Affiliates Limited

Trust Company Complex, Ajeltake Road, Ajeltake Island, Majuro, Republic of the Marshall Islands, MH 96960

Compliance and AML contact: compliance@spend.net

Confidential whistleblowing: compliance@spend.net (marked "Whistleblowing — Confidential")

General enquiries: support@spend.net