AML/KYC Policy

Anti-Money Laundering and Know Your Customer Policy

This Anti-Money Laundering (AML) and Know Your Customer (KYC) Policy has been adopted by SMART ENERGY PROVIDER LLC to make sure that the Smart Energy Pays platform is not used for money laundering, terrorist financing, sanctions evasion or other illegal financial activity, and that we comply with all applicable U.S. laws and regulations. We review and update this policy regularly to reflect legal developments and best practices.

Field	Value
Company	SMART ENERGY PROVIDER LLC, a Florida limited liability company (Florida document number L25000037694), 101 NE 43 St, Miami, FL 33137
Platform	Smart Energy Pays (www.smartenergypays.us and the Smart Energy Pays mobile app)
Version	2.0 (U.S. version)
Effective Date	October 01, 2026
Policy Owner	BSA/AML Compliance Officer
Approved By	Chief Executive Officer

1. Introduction

SMART ENERGY PROVIDER LLC ("Smart Energy Pay", "we", "us" or "our") is a financial technology company that operates the Smart Energy Pays platform in the United States. Through the platform, customers can hold and convert supported digital assets, send and receive U.S. dollar payments, and use the Smart Energy Pays Visa® Card, which is issued by a licensed bank partner.

This policy forms part of our BSA/AML and Sanctions Compliance Program. It is designed to comply with applicable U.S. laws, including:

- the Bank Secrecy Act (BSA), as amended by the USA PATRIOT Act, and its implementing regulations administered by the Financial Crimes Enforcement Network (FinCEN);
- U.S. economic sanctions administered by the Office of Foreign Assets Control (OFAC);
- applicable state money transmission and AML requirements; and
- the AML and sanctions requirements of our card issuing bank, card program partner, banking partners and Visa.

We also follow the recommendations of the Financial Action Task Force (FATF), including for virtual assets.

We work closely with our bank and card program partners, who run their own AML and sanctions programs. We share information with them as required by law and by our agreements.

2. Definitions

Term	Definition
Beneficial Owner	Each individual who, directly or indirectly, owns 25% or more of a legal entity customer, and one individual with significant responsibility to control or manage the entity (for example, a CEO, managing member or general partner).

Customer Identification Program (CIP)	Our procedures for collecting and verifying the identity of each customer before opening an Account.
Customer Due Diligence (CDD)	Understanding the nature and purpose of the customer relationship, building a customer risk profile, and monitoring the relationship on an ongoing basis.
Enhanced Due Diligence (EDD)	Additional checks applied to higher-risk customers and transactions, such as verifying source of funds and source of wealth.
Politically Exposed Person (PEP)	A person who holds or has held a prominent public function, including senior foreign political figures, as well as their immediate family members and close associates. This includes heads of state, senior politicians, senior judges, senior military officers and senior executives of state-owned enterprises.
Sanctioned Jurisdiction	Any country or region subject to comprehensive U.S. sanctions administered by OFAC, as updated from time to time.
Sanctioned Person	Any person or entity on the OFAC Specially Designated Nationals and Blocked Persons List or another U.S. government sanctions list, or owned 50% or more by one or more such persons.
Prohibited Jurisdiction	Any jurisdiction where we do not offer services because of legal restrictions or high risk, including U.S. states and territories where the Smart Energy Pays program is not available.
High-Risk Jurisdiction	Any jurisdiction identified by FATF, FinCEN or Smart Energy Pay as presenting significant money laundering or terrorist financing risk.

3. Initial and Ongoing Screening

We perform due diligence on every customer at onboarding and throughout the relationship. This includes:

- screening customers, beneficial owners and counterparties against OFAC and other sanctions lists, PEP lists and adverse media at onboarding and on an ongoing basis;
- screening digital asset addresses using blockchain analytics, to detect links to sanctioned addresses, scams, darknet markets and other illicit activity; and
- blocking access from Sanctioned and Prohibited Jurisdictions using IP address, device and location checks.

Suspicious or high-risk activity may result in refused or delayed transactions, restriction or closure of the Account, the blocking or rejecting of funds as required by OFAC rules, and reporting to the authorities.

4. KYC Identification Procedures

We apply a risk-based approach and verify customer identities using reliable, independent sources before opening an Account.

Customer type	Information we collect	How we verify it
Individuals	Full legal name, date of birth, U.S. residential address, Social Security Number or ITIN, phone number and email address	Valid government-issued photo ID (such as a driver's license, state ID card or passport), liveness selfie, and checks against independent data sources
Legal entities	Legal name, address, EIN, state of formation, nature of business and expected activity	Formation documents, good standing certificate, ownership and control structure, and verification of each Beneficial Owner and the authorized representative as individuals

We also collect information about the purpose of the Account, expected activity, and, where required, source of funds.

Identity verification is performed remotely through our identity verification provider. Where the results are inconclusive or the risk is higher, we apply additional measures, such as a video call, additional documents or certified translations.

5. Ongoing Monitoring of Customers

We regularly review and update customer information, and monitor transactions to make sure they match each customer's risk profile. We reassess customer risk when new information or unusual activity comes to light.

Trigger	Measures applied
Any transaction of USD 1,000 or more	Additional review against the customer's profile. EDD, including source of funds and source of wealth checks, where risk indicators are present
Customers who have deposited USD 10,000 or more in total	Classified as high-value and reviewed at least weekly under EDD
Wire transfers of USD 50,000 or more	Security call with the customer to confirm the purpose of the transaction and that no third party is involved
Unusual activity, red flags or a change in risk profile	Review by Compliance; may lead to EDD, restriction of the Account or reporting

Our monitoring uses automated, real-time rules for ACH, wire, card and digital asset transactions, together with blockchain analytics and review by trained compliance staff, under the oversight of the BSA/AML Compliance Officer. For funds transfers of USD 3,000 or more, we collect, keep and pass on the required originator and beneficiary information (the "Travel Rule") where it applies.

6. Sanctioned, Prohibited and High-Risk Jurisdictions

We maintain lists of Sanctioned, Prohibited and High-Risk Jurisdictions, based on OFAC sanctions programs, FATF and FinCEN publications and our own risk assessment.

Category	Treatment
Sanctioned Jurisdictions and Sanctioned Persons	Not permitted to use our services. Funds are blocked or rejected and reported to OFAC as required
Prohibited Jurisdictions	Not permitted to use our services
High-Risk Jurisdictions	Subject to EDD and senior management approval

7. High-Risk Situations

We apply EDD to high-risk customers, such as PEPs, customers connected to High-Risk Jurisdictions, and customers with unusual or high-value activity. EDD includes:

- senior management approval to open or continue the relationship;
- verification of source of funds and source of wealth;
- more frequent reviews and closer transaction monitoring; and
- additional information on the purpose and expected use of the Account.

8. Record-Keeping

We keep customer identification records, transaction records and records of our due diligence, monitoring and reporting for at least five (5) years, as required by the Bank Secrecy Act, or longer where required by law or by our partners. Identification records are kept for at least five years after the Account is closed. Records are stored securely and can be made available to regulators, law enforcement and our partners as required.

9. BSA/AML Compliance Officer

The BSA/AML Compliance Officer is responsible for implementing and managing this program. The officer:

- oversees customer due diligence, sanctions screening and transaction monitoring;
- investigates escalated alerts and decides on the actions to take;
- makes sure suspicious activity is reported to the relevant authorities and to our partners as required;
- makes sure staff receive AML and sanctions training when they join and at least once a year after that; and
- reports to senior management on the program, and arranges an independent test of the program at least once a year.

10. Reporting

Where we are required to, we file Suspicious Activity Reports (SARs) with FinCEN, generally within 30 calendar days of initial detection, and report blocked or rejected transactions to OFAC within the required timeframes. We also escalate suspicious activity to our card issuing bank, card program partner and banking partners as required by our agreements.

We do not tell customers or any other person that a SAR has been or may be filed. Disclosing a SAR, or the fact that one has or has not been filed, is prohibited by federal law.

11. Contact

Questions about this policy can be sent to legal@smartenergypay.com or to SMART ENERGY PROVIDER LLC, Attn: Compliance, 101 NE 43 St, Miami, FL 33137, United States of America.