Anti-Fraud Policy

Fraud Prevention and Identity Theft Red Flags Program

This document describes the anti-fraud policies and procedures of SMART ENERGY PROVIDER LLC for the Smart Energy Pays platform in the United States.

Table of Contents

- 1. Version Control
- 2. Document Details
- 3. Introduction
- 4. Prevention and Detection Controls
- 5. Handling Suspected Fraud
- 6. Responding to Red Flags
- 7. Reporting, Record Keeping and Training
- 8. Next Update

1. Version Control

Field	Value
Company	SMART ENERGY PROVIDER LLC, a Florida limited liability company (Florida document number L25000037694), 101 NE 43 St, Miami, FL 33137
Version	2.0
Version Description	U.S. version for the Smart Energy Pays platform
Author	Compliance, SMART ENERGY PROVIDER LLC
Reviewer	Compliance Officer
Approved By	Chief Executive Officer
Date Approved	October 02, 2026
Description	Replaces version 1.0. Updated for U.S. law, the U.S. card program and U.S. payment methods.

2. Document Details

2.1. Process Name

Fraud Prevention. This policy covers:

- Introduction and business model
- Organizational commitment
- Terms and definitions
- Prevention and detection controls
- Handling suspected fraud
- Responding to red flags
- Reporting, record keeping and training

2.2. Objective

The purpose of this policy is to prevent, detect and respond to fraud and identity theft connected with account opening, existing accounts, card use and transaction activity on the Smart Energy Pays platform. It is designed to protect our customers, our bank and card program partners, and our business, while still giving customers a fast and high-quality service.

This policy supports our compliance with applicable U.S. laws and requirements, including:

- the Bank Secrecy Act and the USA PATRIOT Act, including customer identification and suspicious activity reporting requirements administered by the Financial Crimes Enforcement Network (FinCEN);
- U.S. economic sanctions administered by the Office of Foreign Assets Control (OFAC);
- the Identity Theft Red Flags Rule under the Fair and Accurate Credit Transactions Act, to the extent it applies to our program;
- the Electronic Fund Transfer Act and Regulation E, in relation to unauthorized electronic fund transfers;
- the Gramm-Leach-Bliley Act, in relation to safeguarding customer information;
- applicable state money transmission, consumer protection and data breach notification laws; and
- Visa rules and the requirements of our card issuing bank and card program partner.

2.3. Description

This document is a reference for our employees, contractors and partners. Under this policy, we:

- identify red flags that may indicate fraud or identity theft, and build them into our controls;
- respond to red flags in a way that prevents and limits harm to customers and to us;
- apply controls that match the level of risk;
- oversee our service providers, including our identity verification provider, card program partner and banking partners;
- track and document our fraud prevention, detection and response activities;
- train staff to apply this policy;
- report to senior management at least once a year on fraud and identity theft activity, including fraudulent account openings, account takeovers, card fraud, scams affecting customers and payment recalls. The report uses information from our internal systems and from our correspondence with law enforcement, bank partners, our card program partner and other external parties; and
- update this policy regularly to reflect new fraud risks, including risks to customers' safety and to the safety and soundness of our program.

2.4. Parent Process

This policy forms part of our Bank Secrecy Act / Anti-Money Laundering (BSA/AML) and Sanctions Compliance Program, and should be read together with our Information Security Policy and Incident Response Plan.

2.5. Ownership

Role	Designation	Department	Contact
Primary owner	Compliance Officer	Compliance	legal@smartenergypay.com
Executive sponsor	Chief Executive Officer	Executive	dd@smartenergypay.com
Technical controls	Chief Technology Officer	Technology	development@smartenergypay.com

2.6. Key Stakeholders

- Compliance and operations staff
- Customer support staff
- Executive management
- Legal counsel
- Our card issuing bank, card program partner and banking partners
- Consumers and business customers

3. Introduction

3.1. Overview

SMART ENERGY PROVIDER LLC ("Smart Energy Pay", "we", "us" or "our") is a financial technology company. It operates the Smart Energy Pays platform in the United States through www.smartenergypays.us and the Smart Energy Pays mobile app. Through the platform, customers can:

- hold, send and receive supported digital assets in custodial wallets;
- convert between supported digital assets and U.S. dollars;
- receive and send U.S. dollar payments by ACH and wire using virtual account details provided by our partners; and
- use the Smart Energy Pays Visa® Card, issued by a licensed bank under a license from Visa U.S.A. Inc., for purchases and ATM withdrawals.

We are not a bank. Card, banking and certain payment services are provided by our licensed bank and card program partners, and we work closely with them to prevent and detect fraud.

Digital asset transactions are fast and usually irreversible, and fraudsters often target customers through investment scams, romance scams and impersonation scams. Fraud prevention is therefore central to how we run our business. Senior management is committed to:

- developing, implementing, overseeing and maintaining this policy;
- training staff so they can recognize and respond to fraud and identity theft; and
- providing effective oversight of our service provider arrangements.

3.2. Terms and Definitions

Term	Definition
Fraud	Any act for gain that uses deception as its main method; a knowing misrepresentation of the truth or concealment of a material fact to induce another person to act to their detriment.
Identity theft	Fraud committed or attempted using another person's identifying information without authority. Identifying information includes a name, Social Security Number, date of birth, government-issued ID number, passport number, phone number, email address or device identifier.
Account takeover	When someone other than the customer gains unauthorized access to a customer's Account, for example through stolen credentials, phishing or SIM swapping.
Authorized push payment scam	When a customer is tricked into sending money or digital assets to a fraudster themselves, for example in an investment, romance or impersonation scam.
Third party	Any person or entity that directs another person to act on their behalf in a financial transaction. This may include third-party investment websites or brokers, fraudulent merchants, or family members or friends of the account holder.
Elder financial exploitation	The illegal or improper use of an older adult's funds or assets, often by someone they know and trust or by a scammer.
Red flag	A pattern, practice or specific activity that may indicate fraud or identity theft.
Identity verification provider	Our third-party provider (currently Sumsub) that captures identity documents, proof of address and a liveness selfie, checks document validity, screens against sanctions, politically exposed persons and adverse media lists, and detects fraud patterns.
Card program partner	The licensed company that, together with the card issuing bank, provides card issuing, processing and program management services for the Smart Energy Pays Card.
Third-party service provider	Any entity that has a business relationship with us or our partners, whether bank or non-bank, affiliated or not, regulated or not, and domestic or foreign. This includes service providers, vendors and suppliers.

4. Prevention and Detection Controls

4.1. Account Opening

- Customer identification and verification of name, address, date of birth and Social Security Number or ITIN, as required by our Customer Identification Program.
- Document verification and a liveness selfie through our identity verification provider.
- Screening against OFAC and other sanctions lists, politically exposed persons lists and adverse media at onboarding and on an ongoing basis.
- Device, IP address and location checks to detect duplicate accounts, VPN or proxy use, and access from restricted locations.
- Only one Personal Account per person.

4.2. Account Access and Account Takeover

- Multi-factor authentication for logins and sensitive actions.
- Alerts to customers when a new device logs in, or when login details, phone number, email address or withdrawal addresses change.
- A cooling-off period, with withdrawals temporarily limited, after high-risk account changes.
- Automatic lock of the Account after repeated failed login attempts.

4.3. Card Fraud Controls

- Real-time authorization rules and fraud scoring, in coordination with our card program partner.
- Card controls in the app, including instant card freeze and unfreeze, and spending limits.
- Real-time transaction notifications to customers.
- Card disputes and unauthorized transaction claims are investigated under the Card Terms and Regulation E, within the required timeframes, together with our card program partner and issuing bank.

4.4. Payment and Digital Asset Transaction Monitoring

- Rules-based and risk-based monitoring of ACH, wire, card and digital asset transactions.
- Blockchain analytics to screen withdrawal addresses and incoming funds for links to scams, sanctioned addresses, darknet markets and other illicit activity.
- Transaction limits based on the customer's verification level, account age and risk profile.
- Manual review of high-risk withdrawals before they are released.

5. Handling Suspected Fraud

5.1. Suspected Fraud Identified by Internal Flags

Our internal controls flag the following possible suspicious activities. Flagged accounts may be restricted until the customer speaks with a trained customer support or compliance agent.

Red flag	How staff handle it
Signs of possible elder financial exploitation or a scam affecting a vulnerable customer, for example an older customer making large, unusual first-time digital asset purchases or withdrawals to a new address	A security call is held to check whether the customer understands the risks of digital assets and whether a third party is directing them. Red flags are escalated to Compliance. Age alone is never the reason for restricting an account.
Customer fails identity verification at all levels	The customer is asked to contact support for help uploading the required documents. If they ask why they failed, a security call is held to check whether they are being coached by a third party.

Account funded from a bank account in a different name	Staff check incoming ACH and wire details for name mismatches, distinguishing legitimate variations (nicknames, middle names) from third-party funding. Third-party funds may be returned to the sender.
Several deposits in a short period followed by an attempt to withdraw within 24 hours of first funding	Withdrawal is held for manual review, including blockchain analytics on the withdrawal address and a security call where needed.
Customer is on the phone, or another person appears, in the liveness selfie	Our identity verification provider flags most cases automatically. Staff review the results, including the liveness selfie, and hold a security call before approving the account.
Login from a new device or location immediately followed by changes to security details or a withdrawal	Withdrawals are paused and the customer is contacted through their verified details to confirm the activity.
Card used in a pattern that matches card testing or compromise	The card is blocked, the customer is notified, and a replacement card is offered once the customer confirms the activity.

5.2. Suspected Fraud Identified Through Customer Support

If red flags appear at any time during an interaction with a customer, staff must escalate their concerns to Compliance. Red flags include when a customer:

- contacts support from an email address or phone number other than the one registered to their Account;
- mentions sending digital assets to a third-party investment website, trading platform or broker, or a person they met online;
- says they do not control the wallet they are sending funds to;
- uses "we" statements, suggesting someone else is instructing them or sharing their Account;
- cannot correctly answer basic identity questions, such as their year of birth;
- says they have been scammed, or are working with a third party who promises returns;
- asks whether a third party is "legitimate", or asks us to reverse a withdrawal to a third party;
- says they already sent a deposit before their Account was verified;
- is unaware of previous transactions on their Account, or asks where their money has gone;
- is in a hurry or under pressure to send money, or has been told to keep the transaction secret; or
- registered with an address that does not match their identity documents.

Staff may also place a hold on any withdrawal they are concerned about. The hold remains until the withdrawal is manually approved by Compliance after a review, which may include blockchain analytics. Compliance reviews all escalated red flags and may request more identity documents, hold a phone or video call with the customer, restrict the Account, or close it.

5.3. Wire Transfers

All incoming and outgoing wire transfers are reviewed by Compliance or by staff with specific compliance training. Enhanced due diligence is performed on each customer's first wire funding and includes:

- sanctions and adverse media checks;
- review of identity documents;
- checking publicly available information about the customer;
- transaction review, including blockchain analytics on any related digital asset activity;
- a security call for wires of USD 50,000 or more, to confirm that no third party is involved and to understand the purpose of the Account and the transactions;
- security calls on later wires where Compliance considers it necessary;
- a video call to confirm the legitimacy of the Account's use, where needed;
- requests for source of funds or source of wealth documents, such as bank statements; and
- escalation to the Compliance Officer for decision, which may lead to the return of the wire and closure of the Account.

5.4. Enhanced Due Diligence

Enhanced due diligence is conducted at least weekly on high-value customers (generally those who have deposited USD 10,000 or more in total) and on other high-risk customers. It includes:

- enhanced sanctions and adverse media checks;
- review of identity documents;
- checking publicly available information about the customer;
- transaction review, including blockchain analytics;
- a security call, if one has not yet been held, to confirm that no third party is involved and to understand the purpose of the Account and the transactions;
- a video call to confirm the legitimacy of the Account's use, where needed;
- requests for source of funds or source of wealth documents, such as bank statements; and
- escalation to the Compliance Officer for decision, which may involve a more detailed conversation with the customer or a request for further proof of funds.

6. Responding to Red Flags

We respond to red flags in proportion to the level of risk. Appropriate responses include, but are not limited to:

Response	When it may be used
Monitor the Account	Low-risk indicators that need watching
Contact the customer	To confirm activity through their verified contact details
Hold or delay a transaction	Pending review of a suspicious deposit, withdrawal or card transaction
Reset credentials and security codes	Suspected account takeover
Freeze or replace the card	Suspected card compromise
Suspend the Account	Until contact is made with the customer and the review is complete
Close the Account and refuse future accounts	Confirmed fraud, identity theft or serious misuse
Return funds to the sender	Funds received from a third party or obtained through fraud, where permitted by law
Notify our partners	Card or banking fraud that affects the card issuing bank, card program partner or banking partners
Report to authorities	Where required, as described in Section 7
No action	Where review shows the activity is legitimate. The decision and reasons are documented.

7. Reporting, Record Keeping and Training

7.1. Suspicious Activity Reporting

Suspicious activity is escalated to the Compliance Officer. Where we are required to, we file Suspicious Activity Reports (SARs) with FinCEN within the required timeframes, generally within 30 calendar days of initial detection. We also escalate suspicious activity to our card issuing bank, card program partner and banking partners as required by our agreements, so that they can meet their own reporting obligations.

SARs, and the fact that a SAR has or has not been filed, are confidential. Staff must never tell a customer or any third party that a SAR has been or may be filed.

7.2. Law Enforcement and Victim Support

We cooperate with lawful requests from law enforcement. Where customers have been the victims of fraud or scams, we encourage them to report it to the FBI's Internet Crime Complaint Center (www.ic3.gov) and the Federal Trade Commission (www.reportfraud.ftc.gov), and we provide reasonable support with their reports.

7.3. Record Keeping

We keep records of fraud alerts, investigations, decisions, customer communications and reports for at least five years, or longer where required by law or by our partners.

7.4. Training

All customer support, operations and compliance staff are trained on this policy when they join and at least once a year after that. Training covers red flag recognition, scam typologies including elder financial exploitation, security calls, escalation procedures and SAR confidentiality.

7.5. Management Reporting

The Compliance Officer reports to senior management at least once a year on the effectiveness of this policy, significant fraud incidents, fraud losses, trends, and any recommended changes.

8. Next Update

This policy is reviewed and updated at least once a year, and sooner if there is a significant change in fraud risks, our products, our partners or applicable law. The review is carried out by the Compliance Officer and approved by senior management.
Next scheduled review: October 2027.