Anti-Fraud

Retail Payment Activities Act

This document describes the Anti-Fraud policies and procedures for Smart Energy Pay Solutions Ltd.

Table of Contents

1. Version Control 2

2. Document Details 2

2.1. Process Name 2

2.2. Objective/Goal 2

2.3. Description 3

2.4. Parent Process 4

2.5. Ownership 4

2.6. Key Stakeholders 4

3. Introduction 5

3.1. Overview 5

3.2. Terms & Definitions 5

4. Operations 7

4.1. Handling 7

5. Next Update 11

1. Version Control

Version	Version Description	Author	Reviewer	Date Approved	Description
1.0	Creation of policy	Phantom Compliance	COO	15-May-2025	Initial creation of document

2. Document Details

This section provides the key details of the document structure and purpose.

2.1. Process Name

Fraud – contains:

- Introduction
- Business Model Brief
- Organizational Commitment
- Terms & Definitions
- Guiding Principles
- Monitoring

2.2. Objective/Goal

The document objective is to outline the requirements for compliance with Canadian regulations, specifically the Proceeds of Crime (Money Laundering) and Terrorist Financing Act. Risks are assessed, strategies to mitigate/transfer/avoid are outlined, and additional aspects of the compliance regime are summarized.

The purpose of the Anti-Fraud Policy is to detect, prevent, and mitigate fraud and identity theft in connection with account openings, as well as activities involving existing accounts and transaction activity. Smart Energy Pay Solutions Ltd has established effective procedures that facilitate the highest quality customer service while maintaining adequate controls to mitigate the inherent risks associated with fraud and identity theft.

2.3. Description

This document provides an internal/external reference for employees and partners to consult at any time.

- Identify relevant red flags for and incorporate those red flags into the Policy
- Respond appropriately to any detected red flags to prevent and mitigate fraud and identity theft
- Mitigate the risk of fraud and identity theft that is commensurate with the degree of risk posed
- Oversee service provider arrangements. (Sumsub, Phantom Compliance, etc)
- Ensure the Policy is updated periodically to reflect changes in risks to customers and to protect the safety and soundness of the customer from fraud and identity theft
- Establish the framework and principles used that guide the development, implementation, and maintenance of the Policy
- Track and document appropriate fraud and identity theft prevention, detection, and mitigation activities
- Train staff to implement, manage, and support the Policy
- Provide a Fraud and Identity Theft Red Flags report to the Senior Management at least annually

- This report contains a high level summary of fraudulent account registration, account takeover, and wire recall activity
- Information is collected from Smart Energy Pay Solutions Ltd admin system and correspondence with law enforcement, processing banks, and other external parties
- Incorporate existing policies and procedures that control reasonably foreseeable risks

2.4. Parent Process

None

2.5. Ownership

	Name	Designation	Dept/Division	Email
Primary	Manny Bains	Chief Compliance Officer	Compliance	manny@phantomcompliance.com

2.6. Key Stakeholders

Key stakeholders in this process include:

- Operational employees
- Executive
- Legal counsel
- Merchants
- Consumers
- Brokers, mandataries, and other clients

3. Introduction

3.1. Overview

Smart Energy Pay Solutions Ltd is a business that provides retail payment services, including merchant services, virtual banking, virtual currency services, fund transfers, and other related payment activities. Privately owned, Smart Energy Pay Solutions Ltd is a money services business providing virtual assets to Canadians and a limited cohort of international customers. Smart Energy Pay Solutions Ltd operates using both self-serve OTC (over-the-counter) and liquidity services for businesses and individuals.

- Development, implementation, oversight, maintenance, and continued administration of the Policy.
- Staff training is necessary to effectively implement, manage, and support the policy to mitigate, and identify risks associated with fraud and identity theft.
- Exercise appropriate and effective oversight of any Service Provider agreements.

3.2. Terms & Definitions

Fraud: Any crime for gain that utilizes deception as its primary methodology. Defined as "a knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment."

Third Party: Any person or entity that directs another person or entity to act on their behalf for a financial activity or transaction. In the context of Smart Energy Pay Solutions Ltd, this could include third-party investment websites or brokers, fraudulent merchant and/or bust-out schemes, family members or friends of the account holder.

SumSub: SumSub is compliance software for capturing identity proof documents, proof of address documents, and a liveness selfie. The service validates document legitimacy, checks for PEP status, sanctions, and negative media, and detects fraudulent patterns.

Phantom Compliance: Phantom Compliance is an outsourced compliance and risk management consultancy that assists Smart Energy Pay Solutions Ltd in developing and implementing policies and procedures in its business. Additionally, Phantom assists in filing regulatory reports and transaction monitoring.

Identity Theft: Fraud committed or attempted using identifying information of another person without authority. Identifying information includes any name or number that may be used to identify a specific individual, including name, social security number, date of birth, government issued identification number, government passport number, or telecommunications identifying information or access device.

Red Flag: A pattern, practice, or specific activity that indicates the possible existence of fraud and/or identity theft.

Third Party Service Provider: Encompasses all entities that have entered into a business relationship with Smart Energy Pay Solutions Ltd or its partners, whether the third party is a bank or non-bank, affiliated or non-affiliated, regulated or non-regulated, domestic or foreign. The term includes service providers, vendors, subsidiaries, suppliers, and similar relationships.

4. Operations

This section outlines the operational aspects of Smart Energy Pay Solutions Ltd's anti-fraud procedures. The company implements various operational controls and procedures to prevent, detect, and respond to potential fraud.

4.1. Handling

Suspected Fraud Identified by Internal Flags

Smart Energy Pay Solutions Ltd internal controls flag the following possible suspicious activities

- Customer is 60+ years old.
- Customer fails all levels of KYC.
- Account funded under a different name or email address.
- Customer makes three or more Interac e-transfer deposits in 24 hours.
- Customer attempts to withdraw within 24 hours of the first funding.
- Customer is on the phone in a liveness selfie or has another person in the liveness selfie.

Internal controls block customer access to the account until they speak to a customer service agent. Staff are trained to handle the above in the following way:

- Staff are trained to handle the above in the following way Requires a security call with customer service staff who assess whether the customer understands virtual currency risks and whether the customer is being instructed by a third party. Any red flags are escalated to compliance. If required, compliance may request a video call or further identity documents.

- Customer is prompted to contact customer service so they might assist customer in uploading the identity documents required.
- Manual verifications of incoming electronic transfers alert staff to name and email address mismatches. Staff are trained to discern between legitimate customers using nicknames, middle names or the like and instances of a third party attempting to access account.
- Customer makes three or more Interac e-transfer deposits in 24 hours and Customer attempts to withdraw within 24 hours of first funding
- SumSub automatically captures most instances and flags these as possibly fraudulent. Customer service staff are trained to review SumSub results including liveness selfies during each customer interaction. If customer contacts customer service to determine why they have not passed KYC, a security call is conducted to determine whether they were being coached on the phone by a third party.

Suspected Fraud Identified Via Customer Service

If at any time during an interaction with a customer red flags present themselves, staff are instructed to escalate their concerns to compliance. These may include:

- Blocking withdrawal/funding of crypto transaction
- Customer attempts to communicate with staff using an email address other than the one registered to their account
- Any instance where staff feel they want to monitor a withdrawal including virtual currency wallet forensics, a flag is placed on the account blocking withdrawal until manually approved
- Customer mentions withdrawing virtual currency to a third party website or investment broker
- Customer mentions they do not have control over the wallet they are sending funds to

- Customer uses "we" statements, possibly indicating someone else is instructing them or they are sharing their account
- Customer cannot correctly answer identity questions such as: What year were you born, what age does that make you?
- Customer contacts customer service and indicates they have been scammed or have been working with a third party
- Customer contacts customer service seeking advice as to whether a third party is "legitimate" or asking us to reverse withdrawal to third party
- Customer indicates they have already sent a deposit when their account has not yet been verified
- Customer states they have been scammed in the past
- Customer is unaware of previous transactions made on their account or asking where their money has gone
- User on phone in a selfie or has another person in their selfie
- User‘s liveness selfie is blurry or very dark, potentially indicating an attempt to bypass this check
- Address used to register Smart Energy Pay Solutions Ltd account does not match the address listed on their identity documents in SumSub

Compliance will review the red flags and may request additional identity documents, a phone call with compliance staff or may permanently close the account

Wire Transaction

All wire transactions are reviewed by compliance or by staff with specific compliance training Enhanced due diligence is performed for each initial wire funding which includes:

- Sanctions & Adverse Media Checks
- KYC document review
- Attempt to identify customer online through publicly available data

- Transaction review including virtual currency forensics
- Security call on wires exceeding $50,000 with customer to confirm no third party action and to identify the purpose of the account / transactions
- Security calls may be conducted on subsequent wire deposits as compliance staff deem necessary
- Video phone call with customer to confirm legitimacy of account usage
- Request for additional documents to prove source of wealth; including bank statements
- Escalation to Chief Compliance Officer to action. This may involve a more in depth conversation with customer or a request for further proof of funds documentation
- Full return of wire and account ban

Enhanced Due Diligence

Enhanced due diligence is conducted weekly on high value customers (generally depositing $10,000+ lifetime) to monitor for suspicious account activity. Enhanced due diligence includes:

- Enhanced Sanctions & Adverse Media Checks
- KYC document review
- Attempt to identify customers online through publicly available data
- Transaction review including virtual currency forensics
- Security call with customer if one has not yet been conducted, to confirm no third party action and to identify the purpose of the account/transactions
- Video phone call with customer to confirm the legitimacy of account usage
- Request for additional documents to prove the source of wealth; including bank statements
- Escalation to Chief Compliance Officer to action. This may involve a more in-depth conversation with customer or a request for further proof of funds documentation

Response To Red Flags

Smart Energy Pay Solutions Ltd orchestrates subjective responses to red flag data that is identified based on the degree of risk associated. Appropriate responses may include, but not be limited to, the following:

- Monitor accounts for evidence of fraud and/or identity theft
- Contact the customer
- Change any passwords, security codes, or other security devices that permit access to an account
- Ban or prevent a new account from being opened
- Suspend an existing account until contact can be made with the customer
- Close an existing account
- Determine no response is warranted under the circumstances

5. Next Update

This policy shall be reviewed and updated annually to ensure its continued relevance and effectiveness. The review will be conducted by the Compliance Officer and approved by senior management.