AML POLICY

Anti-money Laundering Compliance Policy

Money Laundering is conducting or attempting to conduct a financial transaction knowing that the transaction is designed in whole or in part to conceal or disguise the nature, location, source, ownership, or control of the proceeds of specified unlawful activities. We, PointPay, duly registered under the laws of Saint Vincent and the Grenadines under the name of Point Pay LLC, with registration number 1120 LLC 2021, have developed this Anti-Money Laundering Compliance Policy ("AML Policy") in an effort to maintain the highest possible compliance with applicable laws and regulations relating to anti-money laundering in Saint Vincent and the Grenadines and other jurisdictions, where we conduct business.

Policies and Procedures

Our AML Policy has been reviewed and approved by our Ultimate Beneficial Owner (the "UBO"). Our AML Policy is regularly reviewed and, if necessary, revised in an effort to comply with applicable rules, regulations and policies. AML policy mentioned herein shall be regulated by acts and regulations of Financial Intelligence Unit of Saint Vincent and the Grenadines ("FIU") and our AML Policy is subject to its review and approval, if required.

Internal Controls

We have developed robust internal policies, procedures, and controls designed to comply with applicable laws and regulations, some of which are outlined here on this page including, but not limited to, our Customer Identification Program ("CIP"), the filing of Suspicious Activity Reports ("SARs") and Currency Transaction Reports ("CTRs"), as well as other reporting requirements and audits.

Training

All our employees and officers receive ongoing broad-based AML training, as well as position-specific training. They must participate in such trainings for at least every twelve (12) months to ensure that they are familiar with current legislation updates and in compliance with all applicable laws and regulations of Saint Vincent Grenadines. New employees receive training within thirty (30) days of their start date. All documentation, related to compliance training including materials, tests, results, attendance and date are maintained. In addition, our compliance-training program is updated as necessary to reflect current laws and regulations.

Legal Compliance Officer

Our LCO is responsible for developing and enforcing the policies and procedures of our AML Policy. Our LCO is required to report any violations of our AML Policy directly to our CEO and our UBO. In addition, our LCO is responsible for recording and filing SARs, CTRs and performing an AML Policy audit at least annually.

Customer Identification

Our Customer Identity Program ("CIP") is an important part of our AML Policy, and helps us detect suspicious activity in a timely manner and prevent fraud.

Account Opening Process

In order to open an account and use PointPay, your identity must be verified, authenticated, and checked against government watchlists, including the Office of Foreign Assets Control ("OFAC"). Failure to complete any of these steps will result in your inability to use PointPay.

Individual customer — Prior to opening an account for an individual customer, we attempt to collect, verify, and authenticate the following information:

- Full and correct name of person;
- Permanent address;
- Email address;
- Nationality;
- Mobile phone number;
- Social Security Number ("SSN") or any comparable identification number issued by government;
- Date and place of birth ("DOB");
- Proof of identity: copy of first four pages of passport (e.g., driver's license, or government-issued ID), showing the following details: (a) number and country of issuance, (b) issue and expiry date, (c) signature of the person;
- Additional information or documentation at the discretion of our Compliance Team.
- Non-US customers are required to provide an additional proof of identity (e.g., driver's license, passport, or government-issued ID).

If you successfully meet and complete our CIP requirements and do not appear on the OFAC or any other government watchlist, then we will provide you with account opening agreements electronically.

Institutional customer — Prior to opening an account for an institutional customer, we attempt to collect, verify, and authenticate the following information:

- Institution legal name;
- Employer Identification Number ("EIN") or any comparable identification number issued by government;
- Full legal name (of all account signatories and beneficial owners);
- Email address (of all account signatories);
- Mobile phone number (of all account signatories);
- Address (principal place of business and/or other physical location);
- Proof of legal existence (e.g., state certified articles of incorporation or certificate of formation, certified copy of the Memorandum and Articles of Association, location of registered office, proof of good standing, unexpired government-issued business license, trust instrument or other comparable legal documents as applicable);
- Contract information of owners, principals, and executive management (as applicable);
- Proof of identity (e.g., driver's license, passport or government-issued ID) for each individual beneficial owner that owns 10% or more, as well as all account signatories; and
- Identifying information for each entity beneficial owner that owns 10% or more (see individual customer information collected above for more details).

If your institution successfully meets and completes our CIP requirements and neither it nor any of its owners, principals, executive, or managers appear on OFAC or any other governmental watchlist, we will provide you with account opening agreements electronically.

Suspicious Activity/Currency Transaction Reports Opening Process

We file SARs if we know, suspect or have reason to suspect suspicious activities have occurred on PointPay. A suspicious transaction is often one that is inconsistent with a customer's known and legitimate business, personal activities or personal means. We leverage our compliance department,

which performs transaction monitoring to help identify unusual patterns of customeractivity. Our LCO reviews and investigates suspicious activity to determine if sufficient information has been collected to justify the filing of a SAR.

Our LCO maintains records and supporting documentation of all SARs and CTRs that have been filed.

Reporting Requirements

All records are retained for seven (7) years and are readily available upon official request by an applicable examiner, regulator, or law enforcement agency.

AML Policy Audit

- Internal

The LCO is responsible for performing an audit of our AML Policy at least annually and presenting the results to our CEO and UBO.

- Independent

Our UBO oversees the performance of an independent test of our AML Policy at least annually. The LCO is not responsible for the independent test, and the LCO's performance is a subject of the test. Results are sent directly to the UBO for review.