Bank Secrecy Act (BSA)/Anti-Money Laundering (AML)Program

**APPROVED BY**

smartcashpay BSA Officer

smartcashpay Board of Directors

TABLE OF CONTENTS

1. Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Policy 4

2. Change Control Log 4

3. Compliance Date 4

4. Definitions 5

4.1 Financial Crimes Enforcement Network (FinCEN) 5

4.2 Currency Transaction Report (CTR) 5

4.3 Suspicious Activity Report (SAR) 5

5. Purpose 5

6. Applicability and Scope 5

7. Roles/Responsibilities 5

7.1 Board of Directors 5

7.2 Designated Compliance Officer 6

7.3 Smartcashpay Employees and Contractors 6

8. Requirements 6

8.1 Overview 6

8.2 BSA Compliance Officer 7

8.3 BSA/AML Program 7

8.3.1 Registration of Money Services Business (MSB) 7

8.3.2 Know Your Customer (KYC)/Customer Due Diligence (CDD) Policy 7

8.3.3 Surveillance and Monitoring Policy 8

8.3.4 Office of Foreign Assets Control (OFAC) Screening 8

8.3.5 Non-OFAC Watchlist Screening 9

8.3.6 Currency Exchanges of More Than $1,000 9

8.3.7 Monetary Instrument Log 9

8.3.8 Risk Assessment 10

8.3.9 Updates 10

8.3.10 AML Training 10

8.3.11 Independent Testing 11

8.4 Currency Transaction Report (CTR) 11

8.4.1 CTR Record Retention 11

8.5 SAR Program 11

8.5.1 SAR Filing 12

8.5.2 Continued SAR Filing 12

8.5.3 Law Enforcement Notification 12

8.5.4 SAR Record Retention 12

8.5.5 SAR Confidentiality 13

8.6 Record Retention 13

8.7 Law Enforcement Information Requests 13

9. Conflict Resolution/Escalation 13

10. Exceptions 14

11. Review Schedule 14

12. Senior Manager Approval 14

13. Attachments 15

13.1 Sample Currency Exchange Record 15

13.2 Sample Monetary Instrument Log 15

13.3 SAR Retention Checklist 16

13.4 CTR Retention Checklist 16

13.5 Sample Testing Log 16

13.6 FinCEN Guidance FIN-2013-G001 “Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies” (March 18, 2013) 17

13.7 FinCEN MSB Registration 20

13.8 Correspondence with Colorado Department of Regulatory Agencies 21

# Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Policy

It is the policy of Acme, LLC d/b/a Smartcashpay Vending (“Smartcashpay”) to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities by complying with all applicable requirements under the Bank Secrecy Act (BSA) and its implementing regulations.

*Money laundering* is generally defined as “engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets.” Generally, money laundering occurs in three stages. Illicit proceeds first enter the financial system at the "placement" stage, where funds generated from criminal activities are converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other assets, accounts, or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership, and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex.

Smartcashpay’s BSA/AML policies and internal controls are designed to ensure compliance with all applicable BSA regulations and will be reviewed and updated on a regular basis to account for both changes in regulations and changes in Smartcashpay’s business model.

# Change Control Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Change Date** | **Author** | **Summary of Changes** |
| 1.0 | [Month Day, Year] | BSA Officer | *Know Your Customer/Customer Due Diligence Policy*: Identifies customer and transactional information collected and recorded, as well as the verification of customer identification and government filings in accordance with regulatory expectations. The Policy details the risk-based tier system used to determine the specific information and identification to be collected, recorded, and verified. |
| 1.0 | [Month Day, Year] | BSA Officer | *Surveillance/Monitoring Policy*: Identifies alert routines that screen customer and transactional information for potentially suspicious or unusual activity, as well as the process for reviewing the alert routines. |

# Compliance Date

The Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Program was implemented on [Month Day, Year].

# Definitions

## Financial Crimes Enforcement Network (FinCEN)

A Bureau of the United States Department of Treasury charged with implementing and enforcing the Bank Secrecy Act (BSA) and anti-money laundering (AML) regulations.

## Currency Transaction Report (CTR)

A report to be filed electronically with FinCEN when a customer of Smartcashpay transacts over $10,000 cash via single transaction or multiple transactions that aggregate to be over $10,000 in a single day.

## Suspicious Activity Report (SAR)

A report to be filed electronically with FinCEN when Smartcashpay detects unusual or suspicious activity or has reason to believe unusual or suspicious activity has occurred.

# Purpose

The purpose of the BSA/AML Program is to establish a procedure for Smartcashpay to operate in compliance with FinCEN regulations regarding anti-money laundering, suspicious activity, and other reporting responsibilities. On March 18, 2013, FinCEN released guidance requiring persons administrating or exchanging virtual currencies to register as a money services business (MSB), specifically a money transmitter, and thus comply with FinCEN MSB regulatory requirements to establish an AML program, complete certain government filings, and retain records for presentation as required.

*Reference*: FinCEN Guidance FIN-2013-G001 “Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies.” (See Section 13.6 for a copy of the Guidance.)

# Applicability and Scope

FinCEN’s BSA/AML regulatory requirements are applicable to Smartcashpay under FinCEN Guidance FIN-2013-G001. Smartcashpay operates two SMARTCASH kiosks within the state of Colorado. One of the kiosks is a unidirectional or “one-way” kiosk, which exchanges U.S. Dollar-denominated cash for SMARTCASH-denominated cryptocurrency. The other is a bidirectional or “two-way” kiosk, which exchanges both U.S. Dollar-denominated cash for SMARTCASH-denominated cryptocurrency and, conversely, SMARTCASH-denominated cryptocurrency for U.S. Dollar-denominated cash. The provision of these services meets the definition of a money services business (MSB) as defined by FinCEN.

# Roles/Responsibilities

The roles and responsibilities applicable to Smartcashpay’s BSA/AML compliance are as follows:

## Board of Directors

Smartcashpay’s Board of Directors (“Board”) is responsible for approving the BSA/AML Program and associated initiatives. The Board also oversees the Compliance Officer and overall performance of the initiatives associated with the BSA/AML Program, including day-to-day operations, training, monitoring, and updates.

## Designated Compliance Officer

Smartcashpay’s designated Compliance Officer is responsible for ensuring the following:

(1) The BSA/AML Program is developed and implemented effectively.

(2) The BSA/AML Program is updated as necessary.

(3) Smartcashpay provides ongoing training of appropriate persons concerning their responsibilities under the BSA/AML Program.

(4) Smartcashpay uses independent testing to monitor and maintain the BSA/AML Program.

The Designated Compliance Officer is responsible for overseeing the analysis and disposition of any attempted or completed transactions that raise AML concerns. The Designated Compliance Officer is responsible for analysis and disposition of any attempted or completed transactions that may require reporting to FinCEN, including, but not limited to, Suspicious Activity Report (SAR) filings and Currency Transaction Report (CTR) filings. Furthermore, the Designated Compliance Officer is responsible for analysis and disposition of any attempted or completed transactions that raise an obligation to file a report to governmental officials or law enforcement. The Designated Compliance Officer is responsible for providing Smartcashpay with interpretations of the requirements of the BSA/AML Program and for resolving conflicts that may arise thereto.

## Smartcashpay Employees and Contractors

Smartcashpay must comply with legal and regulatory requirements designed to detect and prevent money laundering and terrorist financing activities. The AML Program states what employees and contractors must do in order to fulfil Smartcashpay compliance obligations. Failure to follow the AML Program or supporting policies and procedures thereto violates Smartcashpay policy and may violate the law. Violation of this program may result in termination of employment or contractual relationship. Violation of the law may result in civil penalties and/or criminal prosecution.

In connection with their duties, employees, contractors, and volunteers of Smartcashpay will thoroughly consider whether attempted or completed transactions are potentially suspicious or unusual and escalate any such instances to the Dedicated Compliance Officer within one (1) business day.

# Requirements

## Overview

As stated in previous sections, Smartcashpay is required to:

(1) Designate a Compliance Officer for the purposes of the BSA/AML Program

(2) Develop and implement a written anti-money laundering program reasonably designed to prevent Smartcashpay from being used to facilitate money laundering or terrorist financing

(3) File reports regarding certain transactions (e.g., currency in excess of $10,000)

(4) File reports of suspicious or unusual activity

(5) Engage in monitoring, testing, and training relating to the BSA/AML Program

(6) Regularly update the policies associated with the BSA/AML Program

(7) Respond to information requests from FinCEN and/or law enforcement

(8) Take other steps, as required, to establish and maintain compliance with FinCEN regulations.

## BSA Compliance Officer

Smartcashpay hereby designates John Q. Public as the Dedicated Compliance Officer for the purposes of the BSA/AML Program.

## BSA/AML Program

Smartcashpay hereby establishes a written BSA/AML Program. Broadly speaking, the goals of the BSA/AML Program are as follows:

(1) Assess the universe of transactions in which Smartcashpay engages

(2) Develop an understanding of the attributes of the transactions in order to differentiate between routine, commonplace transactions in which Smartcashpay engages, and suspicious or unusual transactions that may warrant SAR filing

(3) Develop a culture and process within Smartcashpay to identify transactions that may warrant escalation to the BSA Compliance Officer

(4) Adjust the BSA Program, as necessary, to maintain compliance with evolving requirements.

### Registration of Money Services Business (MSB)

**Federal**

Smartcashpay is registered with FinCEN as a money services business (MSB) in accordance with “Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies” (FIN-2013-G001). Therein, Smartcashpay is registered to conduct money transmitter activities within the state of Colorado. The registration date of record for Smartcashpay is June 22, 2015. Renewal of MSB registration is due within two (2) calendar years or sooner under certain circumstances as identified by FinCEN. (See Section 13.7 for FinCEN MSB registration.)

**State**

Smartcashpay is required under the terms of its FinCEN registration to obtain state-level licensure from the state(s) within which it maintains operations. Smartcashpay currently maintains its operations exclusively within Colorado. Through its ongoing correspondence with the Colorado Department of Regulatory Agencies (DOR), Smartcashpay has requested that the agency make a determination as to whether its business activities would or would not require state money transmitter licensure under existing Colorado law. (See Section 13.8 for Correspondence with Colorado Department of Regulatory Agencies.)

### Know Your Customer (KYC)/Customer Due Diligence (CDD) Policy

Smartcashpay established a KYC/CDD Policy in order to mitigate the risk of being used, intentionally or unintentionally, by criminal elements for money laundering activities. The KYC/CDD Policy enables Smartcashpay to know and understand its customer and his/her financial dealings.

The KYC/CDD Policy identifies the specific customer and transaction information collected and recorded, as well as the verification of customer identification and government filings in accordance with regulatory expectations. (See Know Your Customer/Customer Due Diligence Policy.)

### Surveillance and Monitoring Policy

Smartcashpay established a Surveillance and Monitoring Policy to identify and flag potential suspicious or unusual activity for review and provide for the timely SAR filing of such activity if ultimately determined suspicious or unusual. The Surveillance and Monitoring Policy identifies specific alert routines developed to screen customer and transactional information for potentially suspicious or unusual activity. The alert routines monitor customers for unusual size, volume, or pattern of transactions, taking into account risk factors and “red flags” appropriate to Smartcashpay’s business model. (See Surveillance and Monitoring Policy.)

### Office of Foreign Assets Control (OFAC) Screening

The Office of Foreign Assets Control (OFAC) of the United States Department of Treasury administers and enforces economic and trade sanctions against targeted foreign countries and groups of individuals, terrorism sponsoring organizations, and international narcotics traffickers based on U.S. foreign policy and national security goals.

#### Specially Designated Nationals (SDN)

Smartcashpay screens users against OFAC’s Specially Designated Nationals (SDN) List. In the event a match has been determined, Smartcashpay will contact OFAC via hotline, as well as refuse any pending or future transactions.

Smartcashpay monitors financial transactions performed by or through its network and agents to detect those that involve any entity or person subject to OFAC laws and regulations.

In general, OFAC regulations require the following:

* Blocking accounts and other property of specified countries, entities, and individuals
* Prohibiting or rejecting unlicensed trade and financial transactions with specified countries, entities, and individuals.

In the event a match has been determined, Smartcashpay will contact OFAC via hotline, as well as refuse any pending or future transactions.

#### Sanctions Programs and Country Information

Smartcashpay screens user information and transactional information to determine if it involves individuals and entities with ties to OFAC sanctioned geographic regions and governments (e.g., address and government-issued identification). OFAC administers a number of U.S. economic sanctions and embargoes that target geographic regions and governments. Some programs are comprehensive in nature, block the government, and include broad-based trade restrictions, while others target specific individuals and entities.

Smartcashpay shall refer to the “[Sanctions Programs and Country Information](https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx)” page on the official website of the Office of Foreign Assets Control for information on specific programs.

In general, OFAC regulations require the following:

* Blocking accounts and other property of specified countries, entities, and individuals
* Prohibiting or rejecting unlicensed trade and financial transactions with specified countries, entities, and individuals.

In the event a match has been determined, Smartcashpay will contact OFAC via hotline, as well as refuse any pending or future transactions.

|  |
| --- |
|  |

### Non-OFAC Watchlist Screening

Smartcashpay monitors financial transactions performed by or through its kiosks to detect those that involve any entity or person subject to the following watchlists:

* United States Bureau of Industry and Security
* United States Bureau of International Security and Nonproliferation
* United States Directorate of Defense Trade Controls
* United States Central Intelligence Agency – Chiefs of State and Cabinet Members
* United Kingdom – Her Majesty’s Treasury
* Canada – Office of the Superintendent of Financial Institutions
* European Union – European External Action Services
* Australia – Department of Foreign Affairs and Trade
* United Nations
* Japan – The Ministry of Economy
* China – State Secretariat for Economic Affairs

In the event a match has been determined, Smartcashpay will refuse any pending or future transactions and report the transaction, as prescribed.

### Currency Exchanges of More Than $1,000

Smartcashpay will record each exchange of customer U.S. Dollar-denominated cash for SMARTCASH-denominated cryptocurrency totaling more than $1,000, and each exchange of customer SMARTCASH-denominated cryptocurrency for U.S. Dollar-denominated cash totaling more than $1,000. This record includes both customer and transaction information. (See Section 13.1 for a Sample Currency Exchange Record.)

### Monetary Instrument Log

Smartcashpay will record each exchange of customer U.S. Dollar-denominated cash for SMARTCASH-denominated cryptocurrency totaling $3,000-$10,000 inclusive, and each exchange of SMARTCASH-denominated cryptocurrency for U.S. Dollar-denominated cash totaling $3,000-$10,000 inclusive. This record includes customer and transaction information, as well as government-issued identification and verification information. (See Section 13.2 for a Sample Monetary Instrument Log.)

### Risk Assessment

Smartcashpay has undertaken a Risk Assessment to identify its BSA/AML risk profile, which is the first step in designing tailored controls to mitigate risks and identify gaps in existing controls. The Risk Assessment examined the composition of Smartcashpay’s customer base, geographic footprint, and products and services. The Risk Assessment will assist the Board in understanding where risks related to BSA/AML compliance lie. The assessment included: (a) an evaluation of the adequacy and appropriateness of the policies, procedures, and controls established by Smartcashpay in order to comply with the Bank Secrecy Act and mitigate the associated risk; (b) identification of any significant gaps or weaknesses; and (c) recommendations for improvements that will serve to strengthen Smartcashpay’s overall BSA/AML Compliance Program. (See BSA Risk Assessment.)

### Updates

Smartcashpay will update the BSA/AML Program on an annual basis, at minimum, to ensure compliance with regulatory requirements and adaptation to evolving risk.

### AML Training

Smartcashpay mandates all employees and contractors participate, complete, and adhere to its BSA/AML training as a condition of continued employment. To that end, Smartcashpay has developed and implemented a training program that requires all employees and contractors to be trained as follows:

(1) Every new employee and contractor must be trained on Smartcashpay’s compliance policies and procedures before the employee commences work.

(2) The employee and contractor must be retrained, at minimum, on an annual basis going forward and as required by changing laws and regulations.

The training program will incorporate the requirements of the Bank Secrecy Act (BSA), the USA PATRIOT Act, anti-money laundering laws, and other applicable federal and state laws and regulations. Smartcashpay has tailored its ongoing employee training based on its market capital, customer base, company resources, and other risk-based factors.

Smartcashpay facilitates the training program for all employees and contractors via an e-learning module. The training course materials examine how to identify red flags and signs of money laundering that arise during the course of one's duties; what to do once the risk is identified; individual and collective roles in Smartcashpay’s compliance efforts and how to perform them; record retention obligations; and, the disciplinary consequences (including civil and criminal penalties) for non-compliance with anti-money laundering laws and regulations.

Smartcashpay shall maintain logs of provided training that include the following information:

(1) Date of any training conducted;

(2) Detailed information on the material covered;

(3) List of attendees who completed the AML training, as required by BSA regulations.

Further, whenever possible, Smartcashpay encourages and sponsors officer, employee, and contractor participation in targeted and relevant AML compliance training courses, seminars, conferences, and other opportunities.

### Independent Testing

Smartcashpay will arrange for independent testing of its BSA/AML Program on an annual basis. This testing may be performed by a third-party or by an employee of Smartcashpay other than the Compliance Officer.

Testing performed by Smartcashpay personnel must be conducted by someone other than the BSA Compliance Officer or anyone who engaged in the BSA/AML functions under review. His/her/their qualifications should include, at least, a working knowledge of BSA regulations and regulatory requirements.

As a general matter, independent testing of Smartcashpay’s BSA/AML Program will include, at a minimum: (1) evaluating the overall integrity and effectiveness of Smartcashpay’s BSA/AML Program; (2) evaluating Smartcashpay’s policies pertaining to BSA/AML reporting and recordkeeping requirements; (3) evaluating the implementation and maintenance of Smartcashpay’s KYC/CDD Program; (4) evaluating Smartcashpay’s transactions; (5) evaluating the adequacy of Smartcashpay’s staff training program; (6) evaluating Smartcashpay’s systems, whether automated or manual, for identifying potential suspicious activity; (7) evaluating Smartcashpay’s system for reporting suspicious activity; and (8) evaluating Smartcashpay’s response to previously identified deficiencies, if any. (SeeSection 13.5 for a Sample Testing Log.)

## Currency Transaction Report (CTR)

In addition to any other transaction reporting obligations that apply to Smartcashpay, under the BSA/AML Program, Smartcashpay must file FinCEN Form 112 “Currency Transaction Report” (CTR) in connection with covered transactions. FinCEN Form 112 “Currency Transaction Report” (CTR) is used generally to report cash transactions in excess of $10,000 or a series of related cash transactions that, when aggregated, exceed $10,000. For the purposes of this reporting requirement, *cash* means “U.S. or foreign currency.” Regardless of the type of transaction, there must be over $10,000 cash to trigger the reporting requirement. CTRs are filed electronically with FinCEN. (See Section 13.4 for a CTR Retention Checklist.)

### CTR Record Retention

Smartcashpay will maintain a copy of any CTR it originates, as well as any supporting documentation, for a period of five (5) years from the date of filing.

## SAR Program

Smartcashpay must file a SAR to report transactions that are or appear to be suspicious, unusual, or both, as well as any possible violations of law or regulation.

A SAR must be filed if a transaction meets the following conditions:

(1) The transaction is conducted or attempted by, at, or through Smartcashpay.

(2) The transaction involves or aggregates funds or other assets of at least $2,000.

(3) Smartcashpay knows, suspects, or has reason to suspect the transaction (or a pattern of transactions of which the transaction is a part):

(a) Involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity (including without limitation the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any Federal law or regulation or to avoid any transaction reporting requirement under Federal law or regulation;

(b) Is designed, whether through structuring or other means, to evade any requirements of regulations applicable to Smartcashpay’s BSA/AML obligations or any other regulations promulgated under the Bank Secrecy Act;

(c) Has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and Smartcashpay knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction; or

(d) Involves the use of Smartcashpay to facilitate criminal activity.

### SAR Filing

FinCEN has electronic means for completing and filing SARs. A SAR must be filed no later than thirty (30) calendar days after the date of the initial detection by Smartcashpay of facts that may provide the basis for filing a SAR. If no suspect is identified at the date of such initial detection by Smartcashpay, the SAR may be filed no later than sixty (60) calendar days after the date of initial detection. SARs are filed electronically with FinCEN.

It is the responsibility of the Dedicated Compliance Officer and/or designee to prepare and file all completed SARs with FinCEN in a timely manner.

### Continued SAR Filing

If the activity that warranted the initial SAR filing continues over a period of time, such information must be reported to FinCEN electronically via Continued Activity SAR filing. In accordance with FinCEN guidelines, Continued Activity SAR filings should be filed every ninety (90) calendar days, at minimum. Subsequent guidance permits institutions with SAR requirements, including Smartcashpay, to file SARs for continuing activity after a 90-day review with the filing deadline being 120 calendar days after the date of the previously related SAR filing. Smartcashpay may also file SARs for continuing activity earlier than the 120-day deadline if it believes the activity warrants earlier review by law enforcement.

### 8.5.3 Law Enforcement Notification

In situations requiring immediate attention, such as suspected terrorist financing or ongoing money laundering schemes, Smartcashpay may notify an appropriate law enforcement agency in addition to filing a SAR, as provided within this BSA/AML Program.



### SAR Record Retention

Smartcashpay will maintain a copy of any SAR it originates (including joint reports), as well as any supporting documentation, for a period of five (5) years from the date of filing.

Supporting documentation must be identified as such and maintained by Smartcashpay. Smartcashpay will make all supporting documentation available to FinCEN, or any Federal, State, or local law enforcement agency, or any Federal regulatory authority that examines Smartcashpay for compliance with the Bank Secrecy Act, or any State regulatory authority administering a State law that requires Smartcashpay to comply with the Bank Secrecy Act or otherwise authorizes the State authority to ensure that Smartcashpay complies with the Bank Secrecy Act, upon request. (See Section 13.3 for a SAR Retention Checklist.)

### SAR Confidentiality

A SAR, and any information that would reveal the existence of a SAR, is confidential and shall not be disclosed except as authorized. Smartcashpay, nor any director, officer, employee, or agent of Smartcashpay may disclose a SAR or any information that would reveal the existence of a SAR.

If Smartcashpay and/or any director, officer, employee, or agent of Smartcashpay is subpoenaed or otherwise requested to disclose a SAR or any information that would reveal the existence of a SAR, the recipient of such request must decline to produce the SAR or such information and must notify FinCEN of any such request and the response thereto.

Smartcashpay will cooperate with law enforcement requests for information regarding SARs in connection with law enforcement efforts.

## Record Retention

Smartcashpay will retain BSA/AML records for a period of five (5) years, at minimum. These records will be filed or stored in such a way as to be accessible within a reasonable period of time.

The retention of records includes, but is in no way limited to, the following:

(1) FinCEN Registration — MSBs must maintain copies of their FinCEN registration form and registration number assigned to the business, including any renewal or subsequent forms. (See Section 8.3.1.)

(2) Currency Exchange Record — MSBs must maintain certain records for each currency exchange in excess of $1,000. (See Section 8.3.6.)

(3) Monetary Instrument Log — MSBs must maintain certain information for each purchase of monetary instruments, such as currency, $3,000-$10,000, regardless of the method of payment. (See Section 8.3.7.)

## Law Enforcement Information Requests

FinCEN requires Smartcashpay to comply with information sharing requests regarding accounts and transactions. In the event Smartcashpay receives such a request, Smartcashpay will respond to the request in a timely manner and cooperate completely and thoroughly with FinCEN’s inquiry.

# Conflict Resolution/Escalation

In the event of a question regarding the operation or implementation of the BSA/AML Program, or in the event Smartcashpay staff require an interpretation relating to the Program, the conflict or interpretation request will be escalated to the BSA Compliance Officer, who will resolve the conflict or provide the interpretation.

# Exceptions

There are no exceptions permitted to the BSA/AML Program.

# Review Schedule

Smartcashpay’s BSA/AML Program will be reviewed and updated, at minimum, on an annual basis. Smartcashpay will review and update its BSA/AML Program following any material changes to business operations, company ownership, or both.

# Senior Manager Approval

Smartcashpay’s BSA/AML Program must be approved in writing by a member of Senior Management.

Senior Management has approved this BSA/AML Program in writing as reasonably designed to achieve and monitor Smartcashpay’s ongoing compliance with the requirements of the Bank Secrecy Act (BSA) and the implementing regulations thereunder. This approval is indicated by the signature below.

Signed:

Name:

Title:

Date:

# Attachments

## Sample Currency Exchange Record

|  |  |
| --- | --- |
| Customer Name |  |
| Customer Email Address |  |
| Customer SMARTCASH Address |  |
| Transaction Amount ($) |  |
| Transaction Date |  |

## Sample Monetary Instrument Log

|  |  |
| --- | --- |
| Customer Name |  |
| Customer Email Address |  |
| Customer Phone Number |  |
| Customer Address |  |
| Customer Date of Birth |  |
| Customer Tax Identification Number |  |
| Customer SMARTCASH Address |  |
| Transaction Amount ($) |  |
| Transaction Date |  |
| Description of Customer Identification | Type of ID:  Identification Number:  Issuance Jurisdiction:  Date of Issuance:  Expiration Date: |
| Description of Customer Verification Performed | [Description of the means used to verify the identity of a customer using non-documentary methods.] |
| Resolution of Substantive Discrepancy (if applicable) | [Description of how Smartcashpay resolved any substantive discrepancy noted when verifying customer’s identifying information. These could be misspelled names, inconsistent addresses, inconsistent SSN, etc.] |

## SAR Retention Checklist

|  |  |
| --- | --- |
| Filed SAR | [ ] Copy of completed SAR attached |
| Supporting Documentation | [ ] Copies of all SAR supporting documentation marked “SAR Supporting Documentation”  [ ] SAR supporting documentation attached |

## CTR Retention Checklist

|  |  |
| --- | --- |
| Filed CTR | [ ] Copy of completed CTR attached |
| Supporting Documentation | [ ] Copies of all CTR supporting documentation marked “CTR Supporting Documentation”  [ ] CTR supporting documentation attached |

## Sample Testing Log

|  |  |
| --- | --- |
| Testing Report | |
| Test Type | [ ] Routine Annual Testing  [ ] Other |
| Test Date | [Insert start date and end date of testing.] |
| Testers | [Identify independent testers.] |
| Follow-up items from prior testing | [Describe action items from prior testing, if any, and steps taken to remediate shortcomings.] |
| SAR Review | [Describe results of review of all transactions that were considered for SAR filing to determine compliance with Smartcashpay’s policies and laws and regulations.] |
| AML Review | [Describe results of review of all transactions that were reviewed for elevated AML risk to determine compliance with Smartcashpay’s policies and laws and regulations.] |

## FinCEN Guidance FIN-2013-G001 “Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies” (March 18, 2013)

FIN-2013-G001

|  |
| --- |
|  |
| Issued: | March 18, 2013 |
| Subject: | Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies |

The Financial Crimes Enforcement Network (“FinCEN") is issuing this interpretive guidance to clarify the applicability of the regulations implementing the Bank Secrecy Act ("BSA") to persons creating, obtaining, distributing, exchanging, accepting, or transmitting virtual currencies.1 Such persons are referred to in this guidance as "users," "administrators," and "exchangers," all as defined below.2 A user of virtual currency is **not** an MSB under FinCEN's regulations and therefore is not subject to MSB registration, reporting, and recordkeeping regulations. However, an administrator or exchanger is an MSB under FinCEN's regulations, specifically, a money transmitter, unless a limitation to or exemption from the definition applies to the person. An administrator or exchanger is not a provider or seller of prepaid access, or a dealer in foreign exchange, under FinCEN's regulations.

**Currency vs. Virtual Currency**

            FinCEN's regulations define currency (also referred to as "real" currency) as "the coin and paper money of the United States or of any other country that [i] is designated as legal tender and that [ii] circulates and [iii] is customarily used and accepted as a medium of exchange in the country of issuance."3 In contrast to real currency, "virtual" currency is a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction. This guidance addresses "convertible" virtual currency. This type of virtual currency either has an equivalent value in real currency, or acts as a substitute for real currency.

**Background**

            On July 21, 2011, FinCEN published a Final Rule amending definitions and other regulations relating to money services businesses ("MSBs").4 Among other things, the MSB Rule amends the definitions of dealers in foreign exchange (formerly referred to as "currency dealers and exchangers") and money transmitters. On July 29, 2011, FinCEN published a Final Rule on Definitions and Other Regulations Relating to Prepaid Access (the "Prepaid Access Rule").5 This guidance explains the regulatory treatment under these definitions of persons engaged in virtual currency transactions.

**Definitions of User, Exchanger, and Administrator**

            This guidance refers to the participants in generic virtual currency arrangements, using the terms "user," "exchanger," and "administrator."6 A *user* is a person that obtains virtual currency to purchase goods or services.7 An *exchanger* is a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency. An *administrator* is a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency.

**Users of Virtual Currency**

            A user who obtains convertible virtual currency and uses it to purchase real or virtual goods or services is **not** an MSB under FinCEN's regulations.8 Such activity, in and of itself, does not fit within the definition of "money transmission services" and therefore is not subject to FinCEN's registration, reporting, and recordkeeping regulations for MSBs.9

**Administrators and Exchangers of Virtual Currency**

            An administrator or exchanger that (1) accepts and transmits a convertible virtual currency or (2) buys or sells convertible virtual currency for any reason is a money transmitter under FinCEN's regulations, unless a limitation to or exemption from the definition applies to the person.10 FinCEN's regulations define the term "money transmitter" as a person that provides money transmission services, or any other person engaged in the transfer of funds. The term "money transmission services" means "the acceptance of currency, funds, or other value that substitutes for currency from one person *and* the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means."11

            The definition of a money transmitter does not differentiate between real currencies and convertible virtual currencies. Accepting and transmitting anything of value that substitutes for currency makes a person a money transmitter under the regulations implementing the BSA.12 FinCEN has reviewed different activities involving virtual currency and has made determinations regarding the appropriate regulatory treatment of administrators and exchangers under three scenarios: brokers and dealers of e-currencies and e-precious metals; centralized convertible virtual currencies; and de-centralized convertible virtual currencies.

***a. E-Currencies and E-Precious Metals***

            The first type of activity involves electronic trading in e-currencies or e-precious metals.13 In 2008, FinCEN issued guidance stating that as long as a broker or dealer in real currency or other commodities accepts and transmits funds solely for the purpose of effecting a *bona fide* purchase or sale of the real currency or other commodities for or with a customer, such person is not acting as a money transmitter under the regulations.14

            However, if the broker or dealer transfers funds between a customer and a third party that is not part of the currency or commodity transaction, such transmission of funds is no longer a fundamental element of the actual transaction necessary to execute the contract for the purchase or sale of the currency or the other commodity. This scenario is, therefore, money transmission.15 Examples include, in part, (1) the transfer of funds between a customer and a third party by permitting a third party to fund a customer's account; (2) the transfer of value from a customer's currency or commodity position to the account of another customer; or (3) the closing out of a customer's currency or commodity position, with a transfer of proceeds to a third party. Since the definition of a money transmitter does not differentiate between real currencies and convertible virtual currencies, the same rules apply to brokers and dealers of e-currency and e-precious metals.

***b. Centralized Virtual Currencies***

            The second type of activity involves a convertible virtual currency that has a centralized repository. The administrator of that repository will be a money transmitter to the extent that it allows transfers of value between persons or from one location to another. This conclusion applies, whether the value is denominated in a real currency or a convertible virtual currency. In addition, any exchanger that uses its access to the convertible virtual currency services provided by the administrator to accept and transmit the convertible virtual currency on behalf of others, including transfers intended to pay a third party for virtual goods and services, is also a money transmitter.

            FinCEN understands that the exchanger's activities may take one of two forms. The first form involves an exchanger (acting as a "seller" of the convertible virtual currency) that accepts real currency or its equivalent from a user (the "purchaser") and transmits the value of that real currency to fund the user's convertible virtual currency account with the administrator. Under FinCEN's regulations, sending "value that substitutes for currency" to another person or to another location constitutes money transmission, unless a limitation to or exemption from the definition applies.16 This circumstance constitutes transmission **to another location**, namely from the user's account at one location (e.g., a user's real currency account at a bank) to the user's convertible virtual currency account with the administrator. It might be argued that the exchanger is entitled to the exemption from the definition of "money transmitter" for persons involved in the sale of goods or the provision of services. Under such an argument, one might assert that the exchanger is merely providing the service of connecting the user to the administrator and that the transmission of value is integral to this service. However, this exemption does not apply when the only services being provided are money transmission services.17

            The second form involves a *de facto* sale of convertible virtual currency that is not completely transparent. The exchanger accepts currency or its equivalent from a user and privately credits the user with an appropriate portion of the exchanger's own convertible virtual currency held with the administrator of the repository. The exchanger then transmits that internally credited value to third parties at the user's direction. This constitutes transmission to **another person**, namely each third party to which transmissions are made at the user's direction. To the extent that the convertible virtual currency is generally understood as a substitute for real currencies, transmitting the convertible virtual currency at the direction and for the benefit of the user constitutes money transmission on the part of the exchanger.

***c. De-Centralized Virtual Currencies***

            A final type of convertible virtual currency activity involves a de-centralized convertible virtual currency (1) that has no central repository and no single administrator, and (2) that persons may obtain by their own computing or manufacturing effort.

            A person that creates units of this convertible virtual currency and uses it to purchase real or virtual goods and services is a user of the convertible virtual currency and not subject to regulation as a money transmitter. By contrast, a person that creates units of convertible virtual currency and sells those units to another person for real currency or its equivalent is engaged in transmission to another location and is a money transmitter. In addition, a person is an exchanger and a money transmitter if the person accepts such de-centralized convertible virtual currency from one person and transmits it to another person as part of the acceptance and transfer of currency, funds, or other value that substitutes for currency.

**Providers and Sellers of Prepaid Access**

            A person's acceptance and/or transmission of convertible virtual currency cannot be characterized as providing or selling prepaid access because prepaid access is limited to real currencies. 18

**Dealers in Foreign Exchange**

            A person must exchange the currency of two or more countries to be considered a dealer in foreign exchange.19 Virtual currency does not meet the criteria to be considered "currency" under the BSA, because it is not legal tender. Therefore, a person who accepts real currency in exchange for virtual currency, or vice versa, is not a dealer in foreign exchange under FinCEN's regulations.

\* \* \* \* \*

            Financial institutions with questions about this guidance or other matters related to compliance with the implementing regulations of the BSA may contact FinCEN's Regulatory Helpline at (800) 949-2732.

1 FinCEN is issuing this guidance under its authority to administer the Bank Secrecy Act. See Treasury Order 180-01 (March 24, 2003). This guidance explains only how FinCEN characterizes certain activities involving virtual currencies under the Bank Secrecy Act and FinCEN regulations. It should not be interpreted as a statement by FinCEN about the extent to which those activities comport with other federal or state statutes, rules, regulations, or orders.   
2 FinCEN's regulations define "person" as "an individual, a corporation, a partnership, a trust or estate, a joint stock company, an association, a syndicate, joint venture, or other unincorporated organization or group, an Indian Tribe (as that term is defined in the Indian Gaming Regulatory Act), and all entities cognizable as legal personalities." 31 CFR § 1010.100(mm).   
3 31 CFR § 1010.100(m).   
4 *Bank Secrecy Act Regulations - Definitions and Other Regulations Relating to Money Services Businesses,* 76 FR 43585 (July 21, 2011) (the "MSB Rule"). This defines an MSB as "a person wherever located doing business, whether or not on a regular basis or as an organized or licensed business concern, wholly or in substantial part within the United States, in one or more of the capacities listed in paragraphs (ff)(1) through (ff)(7) of this section. This includes but is not limited to maintenance of any agent, agency, branch, or office within the United States." 31 CFR § 1010.100(ff).   
5 *Final Rule - Definitions and Other Regulations Relating to Prepaid Access,* 76 FR 45403 (July 29, 2011),   
6 These terms are used for the exclusive purpose of this regulatory guidance. Depending on the type and combination of a person's activities, one person may be acting in more than one of these capacities.   
7 How a person engages in "obtaining" a virtual currency may be described using any number of other terms, such as "earning," "harvesting," "mining," "creating," "auto-generating," "manufacturing," or "purchasing," depending on the details of the specific virtual currency model involved. For purposes of this guidance, the label applied to a particular process of obtaining a virtual currency is not material to the legal characterization under the BSA of the process or of the person engaging in the process.   
8 As noted above, this should not be interpreted as a statement about the extent to which the user's activities comport with other federal or state statutes, rules, regulations, or orders. For example, the activity may still be subject to abuse in the form of trade-based money laundering or terrorist financing. The activity may follow the same patterns of behavior observed in the "real" economy with respect to the purchase of "real" goods and services, such as systematic over- or under-invoicing or inflated transaction fees or commissions.   
9 31 CFR § 1010.100(ff)(1-7).   
10 FinCEN's regulations provide that whether a person is a money transmitter is a matter of facts and circumstances. The regulations identify six circumstances under which a person is not a money transmitter, despite accepting and transmitting currency, funds, or value that substitutes for currency. 31 CFR § 1010.100(ff)(5)(ii)(A)-(F).   
11 31 CFR § 1010.100(ff)(5)(i)(A).   
12 Ibid.   
13 Typically, this involves the broker or dealer electronically distributing digital certificates of ownership of real currencies or precious metals, with the digital certificate being the virtual currency. However, the same conclusions would apply in the case of the broker or dealer issuing paper ownership certificates or manifesting customer ownership or control of real currencies or commodities in an account statement or any other form. These conclusions would also apply in the case of a broker or dealer in commodities other than real currencies or precious metals. A broker or dealer of e-currencies or e-precious metals that engages in money transmission could be either an administrator or exchanger depending on its business model.   
14 *Application of the Definition of Money Transmitter to Brokers and Dealers in Currency and other Commodities,* FIN-2008-G008, Sept. 10, 2008. The guidance also notes that the definition of money transmitter excludes any person, such as a futures commission merchant, that is "registered with, and regulated or examined by…the Commodity Futures Trading Commission."   
15 In 2011, FinCEN amended the definition of money transmitter. The 2008 guidance, however, was primarily concerned with the core elements of the definition - accepting and transmitting currency or value - and the exemption for acceptance and transmission integral to another transaction not involving money transmission. The 2011 amendments have not materially changed these aspects of the definition.   
16 See footnote 11 and adjacent text.

17 31 CFR § 1010.100(ff)(5)(ii)(F).

18 This is true even if the person holds the value accepted for a period of time before transmitting some or all of that value at the direction of the person from whom the value was originally accepted. FinCEN's regulations define "prepaid access" as "access to funds or the value of funds that have been paid in advance and can be retrieved or transferred at some point in the future through an electronic device or vehicle, such as a card, code, electronic serial number, mobile identification number, or personal identification number." 31 CFR § 1010.100(ww). Thus, "prepaid access" under FinCEN's regulations is limited to "access to funds or the value of funds." If FinCEN had intended prepaid access to cover funds denominated in a virtual currency or something else that substitutes for real currency, it would have used language in the definition of prepaid access like that in the definition of money transmission, which expressly includes the acceptance and transmission of "other value that substitutes for currency." 31 CFR § 1010.100(ff)(5)(i) .   
19 FinCEN defines a "dealer in foreign exchange" as a "person that accepts the currency, or other monetary instruments, funds, or other instruments denominated in the currency, of one or more countries in exchange for the currency, or other monetary instruments, funds, or other instruments denominated in the currency, of one or more other countries in an amount greater than $1,000 for any other person on any day in one or more transactions, whether or not for same-day delivery." 31 CFR § 1010.100(ff)(1).   
12As our response is not in the form of an administrative ruling, the substance of this letter should not be considered determinative in any state or federal investigation, litigation, grand jury proceeding, or proceeding before any other governmental body.

## FinCEN MSB Registration



MSB Registration Status Information

Date: 07/28/2018

MSB Registration Status Information

Date: 11/18/2018

The inclusion of a business on the MSB Registrant Search Web page is not a recommendation, certification of legitimacy, or endorsement of the business by any government agency.

The MSB Registrant Search Web page, which is updated on a weekly basis, contains entities that have registered as Money Services Businesses (MSBs) pursuant to the Bank Secrecy Act (BSA) regulations at 31 CFR 1022.380(a)(f), administered by the Financial Crimes Enforcement Network (FinCEN).

Information contained on this site has been provided by the MSB registrant. FinCEN does not verify information submitted by the MSB. Information provided on this site reflects only what was provided directly to FinCEN. If an error or incomplete information is detected on this site, the registrant should follow the appropriate instructions for correcting a Registration of Money Services Business (RMSB) form.

MSB Registration Number: 31000068347169

Registration Type: Initial Registration

Legal Name: ACME LLC

DBA Name: Smartcashpay

Street Address: 2595 Canyon Blvd., Suite 420

City: Boulder

State: COLORADO

Zip: 80302

MSB Activities:

Money transmitter

States of MSB Activities:

Colorado

All States & Territories & Foreign Flag:

Number of Branches:

Authorized Signature Date: 06/21/2018

Received Date: 06/22/2018

## Correspondence with Colorado Department of Regulatory Agencies

[Insert copies of coorespondences with state regulators]