

*XANSFER INC.
BSA/AML/OFAC
COMPLIANCE PROGRAM:
POLICIES, PROCEDURES,
AND INTERNAL CONTROLS*

Xansfer Inc.

*3300 Central Expy,
STE B
Santa Clara, CA 95051*

Last update: April 3, 2017

Table of Contents

1.	Introduction.....	4
2.	Firm Policy	4
a.	Company Services Description.....	4
b.	BSA/AML and OFAC Requirements	4
c.	Money Laundering Description.....	5
3.	MSB Registration (31 CFR § 1022.380).....	6
a.	Registration.....	6
b.	Registration Records.....	6
c.	Registration Renewal.....	6
d.	Events Requiring Re-registration.....	6
e.	List of Agents.....	7
4.	Risk Management	7
a.	Product & Service Risks	7
b.	Customer & Entity Risks	7
c.	Geographic Location Risks.....	7
5.	Giving AML Information to Federal Law Enforcement Agencies and Other Financial Institutions	8
a.	FinCEN Requests under USA PATRIOT Act Section 314(a)	8
b.	Voluntary Information Sharing with Other Financial Institutions under USA PATRIOT Act, Section 314(b) (31 C.F.R. § 1010.540).....	9
6.	System of Internal Controls	9
a.	Customer Identification Program (31 C.F.R. § 1022.210(d).....	9
	Covered Transactions	9
	Required Customer Information.....	9
	Verifying Information.....	10
	Recordkeeping	10
b.	Know Your Merchant.....	10
c.	Enhanced Customer Due Diligence.....	10
d.	Checking the Office of Foreign Assets Control Listings.....	10
e.	Monitoring Transactions for Suspicious Activity (31 C.F.R. § 1022.320(a)).....	11
	Transaction Reviews.....	11
	Red Flags	11
	Responding to Red Flags and Suspicious Activity	12
f.	Foreign Agents and Counterparties (FinCEN Release No. 2004-01: https://www.fincen.gov/sites/default/files/shared/msbagentadvisory.pdf).....	12
	Review Structure and Risk Profile.....	12
	Monitoring	13

	Corrective Action and Termination	13
7.	AML Compliance Officer Designation and Duties (31 C.F.R. § 1022.210(d)(2))	13
8.	Agent Relationships	14
a.	Transaction Reviews.....	14
b.	AML Program Reviews.....	15
c.	Agent Transactions – BSA Reporting and Recordkeeping	15
d.	Corrective Action and Termination	15
9.	BSA Reporting	15
a.	Use of the BSA E-Filing System	15
b.	Currency Transaction Report (“CTR”) (31 C.F.R. § 1010.311).....	15
	Identification Required (31 C.F.R. § 1010.312).....	16
	Aggregation (31 C.F.R. § 1010.313)	16
c.	Report of Transportation of Currency or Monetary Instruments (“CMIR”) (31 C.F.R. § 1010.340)	16
d.	Report of Foreign Financial Accounts (31 C.F.R. § 1010.350 and 420).....	16
e.	SAR Filing (31 C.F.R. § 1022.320).....	17
f.	Emergency Notification to Law Enforcement by Telephone (31 F.C.R. § 1022.320(b)(3)).....	17
g.	Joint Filing of SARs with Other Financial Institutions (31 C.F.R. § 1022.320)	18
10.	BSA Recordkeeping.....	18
a.	Required Records of Funds Transmittals (31 C.F.R. § 1010.410)	18
b.	Retrievability	20
c.	Additional Records to Be Retained by Dealers in Foreign Exchange (31 C.F.R. § 1022.410)	20
d.	SAR Maintenance and Confidentiality (31 C.F.R. § 1022.320).....	21
11.	Education and Training Program (31 C.F.R. § 1022.210 (d)(3)).....	21
12.	Independent Review of AML Program (31 CFR § 1022.210 (d)(4))	22
13.	Board of Directors Approval	22
14.	Revision History Page to Track Updates	23

1. Introduction

Xansfer Inc. ("Xansfer"), headquartered in Santa Clara, California, provides cross-border, business payment services. In providing these services, Xansfer engages in the following MSB activities: money transmittals and foreign exchange.

Xansfer also maintains a branch office in Hong Kong:

2/F., Capital Trade Center, 62 Tsun Yip Street,
Kwun Tong, Hong Kong SAR

2. Firm Policy

It is the policy of Xansfer 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.

Our anti-money laundering policies, procedures and internal controls (collectively, our "**AML Program**") are reasonably designed to ensure compliance with all applicable BSA regulations and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in our business.

Our AML Program shall be commensurate with the risks posed by the location and size of, as well as the nature and volume of, the financial services provided by our firm.

Our AML Program shall be kept in writing and approved by Board of Directors. We will make copies of our AML Program available for inspection to the Department of the Treasury upon request.

a. Company Services Description

Xansfer Inc. offers cross-border payment solutions among the US, China and Europe. The company utilizes blockchain technology which includes integrating with cryptocurrency exchanges and build smart apps on blockchain. Xansfer Inc. only deals with corporation clients, and prohibits any transactions with individuals.

b. BSA/AML and OFAC Requirements

In her June 12, 2014, Remarks, FinCEN Director Jennifer Shasky Calvery gave this description of the BSA:

As you likely already know, the Bank Secrecy Act, or "BSA," is the common name for a series of statutes and regulations that form this country's anti-money laundering and countering the financing of terrorism laws. Nearly every country around the world has similar laws in place at this point. These laws are meant to protect the integrity of the financial system by leveraging the assistance of financial institutions to make it more

transparent and resilient to crime and security threats, and by providing information useful to law enforcement and others to combat such threats.

The USA PATRIOT Act (2001) and 31 CFR Chapter X (2011) are among the BSA's more recent and prominent statutes and regulations. The USA PATRIOT Act is one of several statutes referenced by the title *Bank Secrecy Act*. 31 CFR Chapter X contains the organized codification of BSA regulations. (The BSA's implementing regulations organized by financial industry.)

As defined in 31 CFR Part 1010.100(ff), MSB activities include (with certain limitations): dealings in foreign exchange; check cashing services; issuance or sales of traveler's checks or money orders; provision of prepaid access services; money transmittal services; certain activities of the U.S. Postal Service; and sales of prepaid access.

Regulations governing these activities are found in 31 CFR Part 1022, *Rules for Money Services Businesses*. These regulations are divided into four main sections:

- 1) Programs (§1022.210). An MSB's AML program must include policies, procedures, and internal controls for:
 - a. Verifying customer identities;
 - b. Filing reports;
 - c. Creating and retaining records;
 - d. Responding to law enforcement requests.
- 2) Report Filings. MSBs are required to file various reports with FinCEN. These filings include reports of suspicious activities (SARs), currency transaction reports (CTRs); MSB registration (MSBR);
- 3) Maintenance of Records; and
- 4) Information Sharing.

A Note about OFAC: As an office of the US Treasury Department, the Office of Foreign Assets Control ("OFAC") administers and enforces economic and trade sanctions against targeted foreign countries, organizations, and individuals. OFAC imposes controls on transactions and freezes assets under US jurisdiction. While OFAC sanctions are not part of the BSA, OFAC screenings are often conducted in conjunction with a financial institution's BSA-compliance activities.

c. Money Laundering Description

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. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is 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 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.

3. MSB Registration (31 CFR § 1022.380)

a. Registration

We are currently registered with FinCEN as an MSB. Our MSB registration number is 31000100918119.

b. Registration Records

We shall retain a copy of the filed MSB registration form and other supporting documentation at the following US address:

**3300 Central Expy, STE B
Santa Clara, CA 95051**

We shall retain these registration documents for a period of at least five years.

c. Registration Renewal

We shall renew our registration by the end (December 31) of the second calendar year following our initial registration and by December 31 of every second calendar year thereafter.

d. Events Requiring Re-registration

If any of the following events occurs during a registration period (more than 180 days before the next renewal date), we shall re-file a registration form with information different from that reported on the form originally filed:

Change in Ownership or Control under State Law. There has been a change in ownership or control of the MSB that requires the MSB to be re-registered under State law.

Transfer of Voting Power or Equity Interest. More than 10 percent of the voting power or equity interest of the MSB has been transferred (except MSBs that must report such transfer to the Securities and Exchange Commission);

Increase in the Number of Agents. The number of agents of the MSB has increased by more than 50 percent.

To re-register, we shall complete and file an RMSB no later than 180 days after the date on which the triggering event occurred.

e. List of Agents

We do not have any agents at this time and it may not apply to our current state. If it applies in the future, we shall prepare and maintain a list of our agents. We shall update this list by January 1 of each year. We shall make our list of agents available to FinCEN, as well as other appropriate law enforcement agencies, including the IRS, upon request. Our agent list shall include:

- Name: The name of the agent, including any trade names or doing-business-as names.
- Address: The address of the agent, including street address, city, state, and ZIP code.
- Type of Services: The type of MSB services the agent provides on our behalf.
- Gross Transaction Amount: A listing of the individual months in the 12 months preceding the date of the agent list in which the agent's gross transaction amount, for financial products or services issued by our firm, exceeded \$100,000.
- Depository Institution: Name and address of any depository institution at which the agent maintains a transaction account for any of the funds received in or for the MSB services the agent provides on our behalf.
- Year Became Agent: The year in which the agent first became our agent.
- Branches: The number of branches and sub-agents the agent has, if any.

4. Risk Management

We have identified our BSA/AML and OFAC risks regarding products & services, customers & entities, and geographic locations.

a. Product & Service Risks

Our own services and third party services that we rely on may fail due to internal or external reasons. Our mitigating methods will make sure the residual risk is under our tolerance.

b. Customer & Entity Risks

Our clients may intend to deceive us by identify fraud or other activities. Our internal control methods and automated system will prevent such activities from happening at the earliest stage.

c. Geographic Location Risks

Our clients may show evidence that they are related to any high-risk locations or jurisdictions. Our enhanced due diligence will identify such relationships, and reject or terminate those clients' accounts accordingly.

We provide a detailed risk analysis table in our risk assessment file.

5. Giving AML Information to Federal Law Enforcement Agencies and Other Financial Institutions

a. FinCEN Requests under USA PATRIOT Act Section 314(a)

As of the latest update to these procedures, FinCEN did not make regular 314(a) requests of most MSBs. Should FinCEN ever make a 314(a) request of our firm, we shall implement the following policies and procedures:

Upon receiving an information request under 31 C.F.R. § 1010.520, we shall designate one person to be the point of contact regarding the request and to receive similar requests for information from FinCEN in the future. When requested by FinCEN, we shall provide FinCEN with the name, title, mailing address, e-mail address, telephone number, and facsimile number of such person, in such manner as FinCEN may prescribe. After providing FinCEN with this contact information, we shall promptly notify FinCEN of any changes to such information.

As required by 31 C.F.R. § 1010.520(a)(3), “upon receiving an information request from FinCEN under [§ 1010.520, we shall] expeditiously search [our] records to determine whether [we maintain] or [have] maintained any account for, or [have] engaged in any transaction with, each individual, entity, or organization named in FinCEN's request.” If we find a match, our AML Compliance Officer will report it to FinCEN via FinCEN's Web-based 314(a) Secure Information Sharing System within 14 days or within the time requested by FinCEN in the request. If the search parameters differ from those mentioned above (for example, if FinCEN limits the search to a geographic location), our AML Compliance Officer will structure our search accordingly.

When we search our records but do not find a matching account or transaction, we will not reply to the 314(a) request. We will maintain documentation that we have performed the required search by printing a search self-verification document from FinCEN's 314(a) Secure Information Sharing System evidencing that we have searched the 314(a) subject information against our records.

We will not disclose the fact that FinCEN has requested or obtained information from us, except to the extent necessary to comply with the information request. Our AML Compliance Officer will review, maintain and implement procedures to protect the security and confidentiality of requests from FinCEN similar to those procedures established to satisfy the requirements of Section 501 of the Gramm-Leach-Bliley Act with regard to the protection of customers' nonpublic information.

We will direct any questions we have about the 314(a) request to the requesting federal law enforcement agency as designated in the request. Unless otherwise stated in the 314(a) request, we will not be required to treat the information request as continuing in nature, and we will not be required to treat the periodic 314(a) Requests as a government provided list of suspected terrorists for purposes of the customer identification and verification requirements.

b. Voluntary Information Sharing with Other Financial Institutions under USA PATRIOT Act, Section 314(b) (31 C.F.R. § 1010.540)

We may share information with other financial institutions regarding individuals, entities, organizations and countries for purposes of identifying and, where appropriate, reporting activities that we suspect may involve possible terrorist activity or money laundering. Before doing so, our AML Compliance Officer will ensure that the firm files with FinCEN an initial notice before any sharing occurs and annual notices thereafter. We will use the notice form found at [FinCEN's Web site](#). Before we share information with another financial institution, we will take reasonable steps to verify that the other financial institution has submitted the requisite notice to FinCEN, either by obtaining confirmation from the financial institution or by consulting a list of such financial institutions that FinCEN will make available. We understand that this requirement applies even to financial institutions with which we are affiliated. As with non-affiliated firms, we will also obtain the requisite notices from affiliates and follow all required procedures.

We will employ strict procedures both to ensure that only relevant information is shared and to protect the security and confidentiality of this information.

We also will employ procedures to ensure that any information received from another financial institution shall not be used for any purpose other than:

- identifying and, where appropriate, reporting on money laundering or terrorist activities;
- determining whether to establish or maintain an account, or to engage in a transaction; or
- assisting the financial institution in complying with performing such activities.

6. System of Internal Controls

a. Customer Identification Program (31 C.F.R. § 1022.210(d))

As a provider of cross-border, business payment services, Xansfer will only deal with business entity customers. Xansfer will not provide services to individual persons.

To satisfy the Customer Identification Program ("CIP") requirements found in 31 C.F.R. § 1022.210(d)(1) and § 1022.410, we shall collect and verify certain identifying information for each business entity who effects a covered transaction with our firm. We shall record customer identification information and the verification methods and results.

Covered Transactions

Following is a list of covered transaction activities in which our firm may engage:

- Foreign exchange.
- Money transmittals.

Required Customer Information

Before effecting any transaction, we will record the name, address and taxpayer identification number of the entity.

Verifying Information

To comply with the requirements of 1022.210(d)(1) and § 1022.410, we will use risk-based procedures to verify the identity of each customer. We may verify the customer's identity by reviewing a formal document, such as: certified articles of incorporation, a government-issued business license, or a financial statement. We may also use an online identity verification service such as Blockscore (<https://blockscore.com/>), FaceID (<https://faceid.com/>), or Qi Cha Cha (<http://www.qichacha.com/>).

Recordkeeping

We will document our verification, including all identifying information provided by a customer, the methods used and results of verification, and the resolution of any discrepancies identified in the verification process. We will keep records containing a description of any document that we relied on to verify a customer's identity, noting the type of document, any identification number contained in the document, the place of issuance, and if any, the date of issuance and expiration date. With respect to non-documentary verification, we will retain documents that describe the methods and the results of any measures we took to verify the identity of a customer. We will also keep records containing a description of the resolution of each substantive discrepancy discovered when verifying the identifying information obtained. We will retain records of all identification information for five years after the date on which the transaction was effected; we will retain records made about verification of the customer's identity for five years after the record is made.

b. Know Your Merchant

Before providing any money transmittal or foreign exchange services to a business entity, Xansfer will verify the legitimacy of the entity. As described above, verification will be performed through our use of an online identity verification system. We shall perform such verification actions to enable us to form a reasonable belief that we know the true identity of each business entity customer.

c. Enhanced Customer Due Diligence

For accounts we have deemed to be high risk using our risk score table and other methodologies, we will conduct enhanced due diligence, and obtain including but not limited to the following information:

- The source of funds;
- The beneficial owners of the business;
- The customers' clients list;
- Financial statements and banking references;
- Contracts or other proof of documents associated with each transaction.

d. Checking the Office of Foreign Assets Control Listings

Although not part of the BSA and its implementing regulations, Office of Foreign Assets Control (OFAC) compliance is often performed in conjunction with AML compliance. OFAC is an office of the U.S. Treasury that administers and enforces economic sanctions and embargoes based on U.S. foreign policy and national security goals that target geographic regions and governments (e.g., Cuba, Sudan and Syria), as well as individuals or entities that could be anywhere (e.g., international narcotics traffickers, foreign terrorists and proliferators of weapons of mass destruction). As part of its enforcement efforts, OFAC publishes a list of Specially Designated Nationals and Blocked Persons (SDN list), which includes names of companies and individuals who are connected with the sanctions targets. U.S. persons are prohibited from dealing with SDNs wherever they are located, and all SDN assets must be blocked.

Before conducting a transaction of any amount, we will check to ensure that a customer does not appear on the SDN list or is not engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by OFAC. To perform these checks, we may use the OFAC's *Sanctions List Search* application found at <https://sanctionssearch.ofac.treas.gov/>. Because the SDN list and listings of economic sanctions and embargoes are updated frequently, we will consult them on a regular basis and subscribe to receive any available updates when they occur. We will also document our reviews.

If we determine that a customer is on the SDN list or there is a possible match or is engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by OFAC, we will reject the money transmittal request and/or block the customer's assets and file a blocked assets and/or rejected transaction form with OFAC within 10 days. We will also call the OFAC Hotline at (800) 540-6322 immediately.

e. Monitoring Transactions for Suspicious Activity (31 C.F.R. § 1022.320(a))

Transaction Reviews

To ensure our attentiveness to money laundering and terrorist financing activities, we will review all transactions conducted or attempted by, at or through our firm (including transactions conducted with agents) involving \$2,000 or more of funds or assets (either individually or in the aggregate).

On a monthly basis, we will complete a transaction review form ("TRF"), on which we will document our reviews. To evidence our compliance with our requirement to identify and report suspicious transactions, we will maintain copies of our TRFs for at least five years from the date of the review.

Red Flags

We will use a Transaction Review Form ("TRF") to document our reviews of transactions. With our TRF, we will consider whether or not a transaction has, at a minimum, any of the red flags identified by FinCEN in its publication: *Money Laundering Prevention: A Money Services Business Guide* (https://www.fincen.gov/sites/default/files/guidance/msb_prevention_guide.pdf):

Red flags that signal possible money laundering or terrorist financing include, but are not limited to:

Customer ID or Information

- Customer uses false ID.
- Two/more customers use similar IDs.
- Customer alters transaction upon learning that he/she must show ID.
- Customer alters spelling or order of his/her full name.

Transactions Below Reporting or Recordkeeping Thresholds

- Customer conducts transactions just below relevant thresholds:
- Currency exchanges just under \$1,000.

Multiple Customers or Locations

- Two or more customers working together to break one transaction into two or more transactions in order to evade the BSA reporting or recordkeeping requirement.
- Customer uses two or more locations or cashiers in the same day in order to break one transaction into smaller transactions and evade the BSA reporting or recordkeeping requirement.

Overt Illegal Customer Conduct

- Customer offers bribes or tips.
- Customer admits to criminal conduct.

Responding to Red Flags and Suspicious Activity

When an employee of the firm detects any red flag, or other activity that may be suspicious, he or she will notify our AML Compliance Officer. Under the direction of the AML Compliance Officer, the firm will determine whether or not and how to further investigate the matter. This may include gathering additional information internally or from third-party sources, contacting the government, and/or filing a SAR.

If the activity is initially deemed potentially suspicious but after review, our AML Compliance Officer decided that it is not reportable, then we will not file a SAR.

f. Foreign Agents and Counterparties (FinCEN Release No. 2004–01:

<https://www.fincen.gov/sites/default/files/shared/msbagentadvisor.pdf>)

We do not have any agents at this time. The following procedures regarding agents may not apply to our current state but may apply in the future.

Before entering into a relationship with any foreign agent or foreign counterparty, and on at least an annual basis after entering into any such relationship, we shall conduct risk-based due diligence and monitoring of activities:

Review Structure and Risk Profile

- Location of agent/counterparty – check FATF guidance regarding risks posed by jurisdiction.
- Ownership of agent/counterparty – run OFAC check against owners
- Require agent/counterparty to be subject to AML requirements in its jurisdiction and that it establish internal controls.
- Use web searches to check for any reports of AML issues with agent/counterparty.
- Review of agent/counterparty's business, the markets it serves, and the extent to which its structure presents an increased risk for money laundering or terrorist financing.
- Review the types and purposes of services to be provided to, and anticipated activity with, the agent/counterparty.
- Consideration of the nature and duration of our relationship with the agent/counterparty.
- Identify material changes in the agent/counterparty's risk profile (ex: ownership, business, or the regulatory scrutiny to which it is subject).

Monitoring

- Review of transactions to identify and, where appropriate, report suspicious transactions, including:
 - unusual wire activity;
 - bulk sales or purchases of sequentially numbered instruments;
 - multiple purchases or sales that appear to be structured, and;
 - illegible or missing customer information.
- Review of agent/counterparty AML program to discern obvious breakdowns in the implementation of the program by the agent or counterparty.
- Review of agent/counterparty activities for signs of structuring or unnecessarily complex transmissions through multiple jurisdictions that may be indicative of layering or of efforts to evade detection.

Corrective Action and Termination

Agent/counterparty deficiencies noted in our due-diligence activities will be reported to the agent/counterparty. The agent/counterparty must promptly respond to and resolve each identified deficiency. Based on our assessment of the risk presented by each identified deficiency, we shall work with the agent/counterparty to set a resolution date.

Should an agent or counterparty fail to respond timely or appropriately to an identified deficiency, or should our management team determine that an identified deficiency presents an unacceptable risk, we shall take immediate actions to temporarily or permanently cease all business activities with the agent or counterparty. We shall take such actions should an agent or counterparty ever demonstrate systemic, willful, or repeated lapses in compliance with our AML procedures or requirements.

7. AML Compliance Officer Designation and Duties (31 C.F.R. § 1022.210(d)(2))

Xansfer has designated Xin Huang as its Anti-Money Laundering Compliance Officer (“**AML Compliance Officer**”), with full responsibility for the firm’s AML Program. As our AML Compliance Officer, Mr. Huang will oversee all aspects of Xansfer’s compliance with AML regulations. Mr. Huang has a working knowledge of the BSA and its implementing regulations and is qualified by experience, knowledge and training. Mr. Huang has Master of Management Science & Engineering degree from Columbia University. He proceeded international accredited investors compliance (review and verification) when he was in Meixin Finance Group, a global investment company based in New York.

The responsibilities of our AML Compliance Officer shall specifically include assuring that:

- Our firm properly files reports, and creates and retains records, in accordance with applicable requirements of the BSA;
- Our AML Program is updated as necessary to reflect current requirements of the BSA, and related guidance issued by the Department of the Treasury; and
- Our firm provides appropriate training and education in accordance with 31 C.F.R. § 1022.210(d)(3).

8. Agent Relationships

Citing 31 CFR § 1022.210(d)(1)(iii), in its March 11, 2016, Guidance, FinCEN explained that, in MSB principal-agent relationships, “each MSB remains independently and wholly responsible for *implementing* adequate AML program requirements.”

FinCEN went on to explain that, as the principal MSB, we must “have procedures in place to identify those agents conducting activities that appear to lack commercial purpose, lack justification, or otherwise are not supported by verifiable documentation. The principal must implement risk-based procedures to monitor the agents’ transactions to ensure that they are legitimate. The procedures must also ensure that, if the agents’ transactions trigger reporting or recordkeeping requirements, the principal handles the information in accordance with regulatory reporting and recordkeeping obligations. In addition, the MSB principal should implement procedures for handling non-compliant agents, including agent contract terminations.”

Recognizing our responsibility in each of these areas, even we do not have any agents at this time and it may not apply to our current state, we have implemented the following policies, procedures, and internal controls if they may apply in the future:

a. Transaction Reviews

We recognize the risks presented to our firm through the actions of our agents. To address these risks, we will monitor the activities of our agents.

As noted below, we will review transactions conducted through our agents. In performing these reviews, we will be attentive to agent activities that appear to lack commercial purpose, lack justification, or otherwise are not supported by verifiable documentation.

As part of these reviews, we will confirm that, for agent transactions which trigger BSA reporting or recordkeeping requirements, we have created the required records and filed the required reports.

b. AML Program Reviews

On at least an annual basis, we will also review the written AML policies and procedures of each of our agents. We will perform these reviews to ensure that our agents have effective AML programs. An effective AML program will address all relevant BSA requirements including: CIP, Transaction Monitoring, BSA Reporting, and Recordkeeping.

c. Agent Transactions – BSA Reporting and Recordkeeping

As specified in this program, Xansfer accepts full responsibility for BSA reporting and recordkeeping requirements related to Xansfer's MSB activities. Whether transactions are conducted directly with us, or whether they are conducted through our agents, we will file all required reports and keep all required records.

d. Corrective Action and Termination

Agent deficiencies noted in our due-diligence activities will be reported to the agent. The agent must promptly respond to and resolve each identified deficiency. Based on our assessment of the risk presented by each identified deficiency, we shall work with the agent to set a resolution date.

Should an agent fail to respond timely or appropriately to an identified deficiency, or should our management team determine that an identified deficiency presents an unacceptable risk, we shall take immediate actions to temporarily or permanently cease all business activities with the agent. We shall take such actions should an agent ever demonstrate systemic, willful, or repeated lapses in compliance with our AML procedures or requirements.

9. BSA Reporting

a. Use of the BSA E-Filing System

We shall use the BSA E-Filing System to submit each SAR, CTR, FinCEN Form 114 (FBAR), and RMSB as applicable.

b. Currency Transaction Report ("CTR") (31 C.F.R. § 1010.311)

We prohibit dealing with currency currently. There is little if not zero chance we make a currency transaction. Should we make such transactions, we shall implement the following policies and procedures:

For each deposit, withdrawal, exchange of currency or other payment or transfer, by, through or to us, which involves a transaction in currency of more than \$10,000 and which is not between our firm and a commercial bank (see § 1010.315), we shall file with FinCEN a CTR. Also, we

will treat multiple transactions involving currency as a single transaction for purposes of determining whether to file a CTR if they total more than \$10,000 and are made by or on behalf of the same customer during any one business day. We shall file a CTR within 15 days following the day on which the reportable transaction occurred. We shall retain a copy of each CTR for a period of five years from the date of the report.

Identification Required (31 C.F.R. § 1010.312)

Before concluding any transaction with respect to which the filing of a CTR is required, we shall verify and record the name and address of the individual presenting the transaction, as well as record the identity, account number, and taxpayer identification number, if any, of any entity on whose behalf such transaction is to be effected. Verification of the identity of an individual who indicates that he or she is an alien or is not a resident of the United States shall be made by passport, alien identification card, or other official document evidencing nationality or residence.

In each instance, the specific identifying information used in verifying the identity of the customer shall be recorded on the report.

Aggregation (31 C.F.R. § 1010.313)

In determining whether or not we are obligated to file any CTR, we shall aggregate all transaction activities.

We shall treat multiple currency transactions as a single transaction if we have knowledge that these transactions are made by or on behalf of any customer and result in either cash in or cash out totaling more than \$10,000 during any one business day.

c. Report of Transportation of Currency or Monetary Instruments (“CMIR”) (31 C.F.R. § 1010.340)

As required by 31 C.F.R. § 1010.340, we shall file a CMIR with the Commissioner of Customs if we discover that we have received or caused or attempted to receive from outside of the U.S. currency or other monetary instruments in an aggregate amount exceeding \$10,000 at one time. We shall file such report within 15 days after receipt of the currency or other monetary instruments.

We shall also file a CMIR if we discover that we have physically transported, mailed or shipped or caused or attempted to physically transport, mail or ship by any means currency or other monetary instruments of more than \$10,000 at one time. We shall file such report at the time of departure, mailing or shipping from the United States.

d. Report of Foreign Financial Accounts (31 C.F.R. § 1010.350 and 420)

As of the date of this program, we have no financial interest in, or signature or other authority over, a bank, securities, or other financial account in a foreign country.

Should we ever have a financial interest in, or signature or other authority over, a bank, securities, or other financial account in a foreign country, we shall report such relationship to the

Commissioner of Internal Revenue for each year in which such relationship exists and shall provide such information as shall be specified in a reporting form prescribed under 31 U.S.C. 5314. The form prescribed under section 5314 is the Report of Foreign Bank and Financial Accounts (FinCEN Form 114 or "FBAR").

We shall file all FBARs with the Commissioner of Internal Revenue on or before June 30 of each calendar year with respect to foreign financial accounts exceeding \$10,000 maintained during the previous calendar year. We shall retain such records for a period of five years and shall keep them at all times available for inspection as authorized by law.

e. SAR Filing (31 C.F.R. § 1022.320)

We will file a SAR with FinCEN for any transactions conducted or attempted by, at or through our firm involving \$2,000 or more of funds or assets (either individually or in the aggregate) where we know, suspect or have reason to suspect that the transaction:

- involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation;
- is designed, whether through structuring or otherwise, to evade any requirements of the BSA regulations;
- serves no business or apparent lawful purpose, and after examining the available facts, including the background and possible purpose of the transaction. we know of no reasonable explanation for the transaction; or
- involves the use of the firm to facilitate criminal activity.

We may voluntarily file a SAR for any suspicious transaction that we believe is relevant to the possible violation of any law or regulation but that is not required to be reported by us under the SAR rule. It is our policy that all SARs will be reported regularly to the Board of Directors and appropriate senior management, with a clear reminder of the need to maintain the confidentiality of the SAR.

We will file a SAR no later than 30 calendar days after the date of the initial detection of the facts that constitute a basis for filing a SAR. The phrase "initial detection" does not mean the moment a transaction is highlighted for review. The 30-day period begins when an appropriate review is conducted and a determination is made that the transaction under review is "suspicious" within the meaning of the SAR requirements. A review must be initiated promptly upon identification of unusual activity that warrants investigation.

f. Emergency Notification to Law Enforcement by Telephone (31 F.C.R. § 1022.320(b)(3))

In situations involving violations that require immediate attention, such as ongoing money laundering schemes, we will immediately call an appropriate law enforcement authority. In addition to local law enforcement authorities, we may also contact FinCEN's Financial Institutions Hotline (866.556.3974) to report transactions relating to terrorist activity. If we notify the appropriate law enforcement authority of any such activity, we must still file a timely SAR.

g. Joint Filing of SARs with Other Financial Institutions (31 C.F.R. § 1022.320)

If we and one or more other party have an obligation to report a transaction, we may file a single SAR jointly with the other party.

When filing jointly, we will ensure that the filed SAR contains all relevant facts, including the name of each party involved in the transaction. We will also ensure that the SAR complies with all instructions applicable to joint filings, and that we keep a copy of the report filed, along with any supporting documentation.

If we determine it is appropriate to jointly file a SAR, we understand that we cannot disclose that we have filed a SAR to any party except the party that is filing jointly. If we determine it is not appropriate to file jointly (e.g., because the SAR concerns the other party or one of its employees), we understand that we cannot disclose that we have filed a SAR to any party.

10. BSA Recordkeeping

We will keep all required records (including CIP records, SAR filings, KYC, Program, policies and procedures, training, training logs, and other required records) for at least five years.

a. Required Records of Funds Transmittals (31 C.F.R. § 1010.410)

In addition to the maintenance of records referenced elsewhere in this program, we shall retain either the original or a copy of each of the following:

For funds transmittals under the Funds Transfer and Travel Rules (31 C.F.R. § 1010.410(e) and (f)), when we are the transmitter's financial institution in funds of \$1,000 or more, we will retain a record of the transmittal order. We will record the following information on the transmittal order:

- the name and address of the transmitter;
- the amount of the transmittal order;
- the execution date of the transmittal order;
- any payment instructions received from the transmitter with the transmittal order;
- any form relating to the transmittal of funds that is completed or signed by the person placing the transmittal order. and
- the identity of the recipient's financial institution.

In addition, we will include on the transmittal order as many of the following items of information as are received with the transmittal order:

- the name and address of the recipient;
- the account number of the recipient;

- any other specific identifier of the recipient; and

In the case of a transmittal order of \$1,000 or more from a transmitter that is not an established customer, in addition to obtaining and retaining the information required by 31 C.F.R. § 1010.410(e)(1)(i), we will follow the criteria specified by § 1010.410(e)(2)(i) and (ii):

- Verify identity of person placing the order.
- Retain a record of the following information of the person placing the order: name, address, tax id number or alien identification number or passport number, and copy of the presented identification.
- If we know that the person placing the order is not the transmitter, we shall retain a record of the transmitter's tax id number or alien identification number or passport number and country of issuance, if known by the person placing the order, or a notation in the record of the lack thereof.

If the transmittal order is not made in person, we shall retain a record of the following:

- Name and address of the person placing the transmittal order, the person's tax id number, alien identification number or passport number and country of issuance, or a notation in the record of the lack thereof, and a copy or record of the method of payment (e.g., check or credit card transaction) for the transmittal of funds.
- If we know that the person placing the transmittal order is not the transmitter, we shall obtain and retain a record of the transmitter's tax id number or alien identification number or passport number and country of issuance, if known by the person placing the order, or a notation in the record of the lack thereof.

For each transmittal order of \$1,000 or more that we accept as a recipient's financial institution for a recipient that is not an established customer, in addition to obtaining and retaining the information required by 31 C.F.R. § 1010.410(e)(1)(iii), we shall also obtain the information required by 31 C.F.R. § 1010.410(e)(3)(i) and (ii):

If the proceeds are delivered in person to the recipient or its representative or agent, we shall

- Verify the identity of the person receiving the proceeds, and
- Retain a record of the name and address, the type of identification reviewed, and the number of the identification document, as well as a record of the person's tax id number or alien identification number or passport number and country of issuance, or a notation in the record of the lack thereof.

If we have knowledge that the person receiving the proceeds is not the recipient, we shall obtain and retain the following:

- a record of the recipient's name and address, as well as the recipient's taxpayer id number or alien identification number or passport number and country of issuance, if known by the person receiving the proceeds, or a notation in the record of the lack thereof.

If the proceeds are delivered other than in person, we shall retain a copy of the check or other instrument used to effect payment, or the information contained thereon, as well as the name and address of the person to which it was sent.

b. Retrievability

Regarding the information that shall be retained under section “a”, above:

As the transmitter’s financial institution, we shall retain information in a format that shall allow us to retrieve the information by reference to the name of the transmitter. If the transmitter is an established customer and has an account used for transmittals of funds, then the information also shall be retrievable by account number.

As the recipient’s financial institution, we shall retain information of our recipient in a format that shall allow us to retrieve the information by reference to the name of the recipient. If the recipient is an established customer and has an account used for transmittals of funds, then the information also shall be retrievable by account number.

c. Additional Records to Be Retained by Dealers in Foreign Exchange (31 C.F.R. § 1022.410)

When conducting foreign exchange transactions, we shall retain either the original or a copy of each of the following:

- Statements of accounts from banks, including paid checks, charges or other debit entry memoranda, deposit slips and other credit memoranda representing the entries reflected on such statements;
- Daily work records, including purchase and sales slips or other memoranda needed to identify and reconstruct currency transactions with customers and foreign banks;
- A record of each exchange of currency involving transactions in excess of \$1,000, including the name and address of the customer (and passport number or taxpayer identification number unless received by mail or common carrier) date and amount of the transaction and currency name, country, and total amount of each foreign currency;
- Signature cards or other documents evidencing signature authority over each deposit or security account, containing the name of the depositor, street address, taxpayer identification number (TIN) or employer identification number (EIN) and the signature of the depositor or of a person authorized to sign on the account (if customer accounts are maintained in a code name, a record of the actual owner of the account);
- Each item, including checks, drafts, or transfers of credit, of more than \$10,000 remitted or transferred to a person, account or place outside the United States;
- A record of each receipt of currency, other monetary instruments, investment securities and checks, and of each transfer of funds or credit, or more than \$10,000 received on any one occasion directly and not through a domestic financial institution, from any person, account or place outside the United States;
- Records prepared or received by us in the ordinary course of business, that would be needed to reconstruct an account and trace a check in excess of \$100 deposited in such account through our internal recordkeeping system to our depository institution, or to supply a description of a deposited check in excess of \$100;

- A record maintaining the name, address and taxpayer identification number, if available, of any person presenting a certificate of deposit for payment, as well as a description of the instrument and date of transaction;
- A system of books and records that will enable us to prepare an accurate balance sheet and income statement.

d. SAR Maintenance and Confidentiality (31 C.F.R. § 1022.320)

We will retain copies of all SARs filed and any supporting documentation for five years from the date of filing the SAR.

We will not notify any person involved in the transaction that the transaction has been reported, except as permitted by the BSA regulations. We understand that anyone who is subpoenaed or required to disclose a SAR or the information contained in the SAR will, except where authorized by FinCEN, decline to produce the SAR or to provide any information that would disclose that a SAR was prepared or filed. We will notify FinCEN of any such request and our response.

We may share information with another financial institution about suspicious transactions in order to determine whether we will jointly file a SAR according to the provisions of Section 4.e (above). In cases in which we file a joint SAR for a transaction that has been handled both by us and another financial institution, both financial institutions will maintain a copy of the filed SAR.

11. Education and Training Program (31 C.F.R. § 1022.210 (d)(3))

Under the direction of our AML Compliance Officer, we will provide ongoing education and training of appropriate personnel. This education and training will occur on at least an annual basis. It will explain the responsibilities of firm personnel under the firm's AML compliance program, including education and training in the detection of suspicious transactions. If we have any branch offices or agents, we will ensure that they receive appropriate training.

Our training will include, at a minimum: (1) how to identify red flags and signs of money laundering that arise during the course of the employees' duties; (2) what to do once the risk is identified (including how, when and to whom to escalate unusual customer activity or other red flags for analysis and, where appropriate, the filing of SARs); (3) what employees' roles are in the firm's compliance efforts and how to perform them; (4) the firm's record retention policy; and (5) the disciplinary consequences (including civil and criminal penalties) for non-compliance with the BSA.

We will develop training in our firm, or contract for it. Delivery of the training may include educational pamphlets, videos, intranet systems, in-person lectures and explanatory memos. We will maintain records to show the names of persons trained, dates of training, and copies of training.

12. Independent Review of AML Program (31 CFR § 1022.210 (d)(4))

The review of our AML compliance program will be performed annually (on a calendar year basis) by Securities Industry Records Services, LLC ("SIRS"), an independent, third-party service provider, or by another, similarly qualified, service provider. We have evaluated SIRS' qualifications to ensure they have a working knowledge of applicable requirements under the BSA and its implementing regulations.

SIRS' CEO, Kevin Klundt, is a Certified Anti-Money Laundering Specialist® ("CAMS") and is a member of the Association of Certified Anti-Money Laundering Specialists ("ACAMS"). He has passed multiple certification examinations and has participated in numerous industry-sponsored regulatory compliance and AML training programs. Mr. Klundt has also held the position of AML Compliance Officer with a BSA-regulated financial institution.

After the completion of each annual, independent review, Board of Directors will review the review report. We will promptly address each of the resulting recommendations and keep a record of how each noted deficiency was resolved.

13. Board of Directors Approval

Board of Directors of Xansfer Inc. has approved this AML compliance program in writing as reasonably designed to achieve and monitor our firm's ongoing compliance with the requirements of the BSA and the implementing regulations under it. This approval is indicated by the signature below.

Signed:



Title:

CEO

Date:

April 3, 2017

14. Revision History Page to Track Updates

February 26, 2017 -- Initial version

March 2, 2017 -- Removed irrelevant parts

March 10, 2017 -- Rephrased several parts

April 3, 2017 -- Reviewed and revised by SIRS