AML Policy & Procedure Guide
2019

The purpose of the guide is to help you, your employees and your business:

- Comply with Bank Secrecy Act (BSA) recordkeeping and reporting requirements;
- Comply with the USA PATRIOT Act;
- Comply with the requirements of the Office of Foreign Assets Control (OFAC) and other anti-money laundering regulations
- Detect and prevent money laundering and terrorist financing, and;
- Identify and report suspicious activity

Your knowledge of the information contained in this guide may help prevent your business from becoming a victim of money laundering and help you comply with federal laws and regulations. Your compliance may help law enforcement agents in their efforts to discover and confine terrorists who illegally launder money.

It is FirsTech's policy to comply with all rules and regulations set forth by the government. We will not do business with anyone who knowingly violates the law. While we cannot take responsibility for you or your employees' compliance with anti-money laundering laws

Contents

Section I
Overview

The Patriot Act which amends the Bank Secrecy Act (BSA), was adopted in response to the September 11, 2001 terrorist attacks. The Patriot Act is intended to strengthen U.S. measures to prevent, detect, and prosecute international money laundering and the financing of terrorism. These efforts include anti-money laundering (AML) tools that impact the banking, financial, and investment communities. Businesses that sell money orders and/or money transfers are subject to the Bank Secrecy Act (BSA), the USA PATRIOT Act, OFAC, other anti-money laundering laws, and to their reporting and recordkeeping obligations.

A business is a Money Service Business (MSB) if it conducts more than $1,000 in business with one person in one or more transactions (in any category of activity listed below) on the same day in one or more of the following services;

- Money Orders
- Travelers Checks
- Check Cashing
- Currency Dealing or Exchange
- OR the business provides Money Transfer services in any amount

Not required to register:

- The U.S. Postal Service
- Any agencies of the United States, of any State, or of any political subdivision of a State.
- An issuer, seller or redeemer of stored value.
- A business that is an MSB solely because it serves as an agent of another MSB. However, if a business that is an agent for another MSB also engages in MSB activities on its own behalf, such as cashing checks on its own behalf for any person of over $1,000 in one or more transactions during a day, the *business is required to register*.
- Banks (including credit unions) and persons registered with and regulated or examined by the Securities and Exchange Commission or Commodity Futures Trading.
- Commissions are not required to register because they are not MSBs. However, if such an entity has a money order division with agents or a money transmission division with agents, those agents may be required to register because they are not agents of an MSB.

Money Services Businesses (MSBs) and their employees who conduct money order sales and money transfer transactions must abide by with all anti-money laundering laws and regulations that apply to them.

Section II
MSB Registration

If a business engages in MSB activities their own behalf, they may be required to register as an MSB with the Financial Crimes Enforcement Network (FinCEN) of the U.S. Department of Treasury. For example, an entity that is sells money orders but performs no other MSB services is not required to register. However, registration would be required if the business also cashes checks for $1,000 or more for any person on any day, in one (1) or more transactions.

The MSB registration form (TD F 90-22.55) must be filed within 180 days after the MSB is established with the Department of Treasury and sent to the address provided on the form. The MSB must retain a copy of the registration form and confirmation letter for five (5) years. Renewal of an MSB registration must occur every 24 months MSBs must re-register if there is:
Change in ownership or control that requires the business to re-register under State law;

- Transfer of more than 10 percent of the voting power or equity interests
- A more than 50 percent increase in the number of agents during the registration period.

Section III
Anti-Money Laundering Compliance Program

The BSA and USA PATRIOT Act require that all MSBs adopt a written anti-money laundering compliance program that is reasonably designed to ensure proper record keeping and reporting of certain transactions and to prevent a business from being used to launder money. At a minimum, an anti-money laundering compliance program must include:
The designation of a Compliance Officer who is responsible for assuring that:

- Policies and procedures are followed
- Procedures are updated as needed
- Training and education are provided
- Reports are properly filed
- Internal policies, procedures and controls for:
- Verifying customer identification
- Filing reports
- Creating and retaining records
- Responding to law enforcement requests
- An ongoing employee training program that: Explains policies and procedures and teaches how to identify suspicious activity

- An independent review of the anti-money laundering program
- The review should take place as needed and be as thorough as needed based on the risks specified to the business.

- The review may be performed by an employee but cannot be the performed by the Compliance Officer.

Establishing an Effective Compliance Program

First, your business *must* designate a Compliance Officer. Every MSB must designate a person to act as the Compliance Officer for the business and will be responsible for making sure the business complies with federal and state law antimony laundering and terrorist financing prevention laws and the policies in this AML Program. This business' Compliance Officer and senior management are and will be responsible for the following:

- Ensuring this business will comply with all federal and state anti-money laundering laws and regulations on a day-to-day basis.

- Ensuring that all current employees who sell money orders are initially trained on how to comply with the applicable anti-money laundering laws and regulations.

- Ensuring new employees who will sell money orders are trained on how to comply with the applicable anti-money laundering laws and regulations before beginning to sell money orders.

- Ensuring that all employees who sell money orders and/or manage this business receive training on anti-money laundering laws and regulations on a regular basis. Documenting all training provided to employees.

- Ensuring that this business' anti-money laundering program is reviewed for effectiveness by someone other than the Compliance Officer periodically.

- Ensuring this business cooperates with law enforcement on anti-money laundering investigations.

- Ensuring the anti-money laundering program is updated as needed to reflect changes in laws and regulations and that employees selling money orders know and understand the changes.

- Ensuring that all reports and records relating to the sale of money orders and Bank Secrecy Act compliance are filed and/or maintained.

Second, your business should formally adopt internal policies, procedures and controls to ensure that you, your employees, and your business are not at risk. The policies,

procedures, and internal controls should be reasonably designed to achieve compliance with the BSA and its implementing rules; policies and procedures should be reasonably expected to detect and cause the reporting of transactions under the Bank Secrecy Act - 31 U.S.C. 5318(g) and the implementing regulations related to this law.

Third, your business must establish an ongoing training program for all employees who will have any involvement with MSB activities. The educations and training should include instructions on the employees' responsibilities under the program, as well as the detections of suspicious transactions. All employees should be required to read this Guide prior to conducting any MSB transactions. In addition, employees should sign your Compliance Program or another form of training documentation that is kept in their personnel file. Employees should also receive periodic updates to their training, particularly when there are changes in regulations.

Fourth, your business should subject its anti-money laundering compliance program to an independent review to assure its adequacy. The scope and frequency of this review should be adjusted to allow for the risk of the financial services provided by your business. This review may be conducted by an officer or employee of your business, but it cannot be conducted by the Compliance Officer.

Finally, it is important that you create recordkeeping files for your Compliance Program. These files should be readily accessible if your business is examined/audited by regulators.

Section IV
Gramm-Leach-Bliley Compliance

Federal law requires every business that collects nonpublic personal information to have a privacy program that complies with the Gramm-Leach-Bliley Act. The following constitutes a Privacy Program which is comprised of several parts, including: Designation of a Privacy Officer, Risk Assessment, Design and implementation of safeguards to limit or control identified risks, Oversee service providers, Evaluation of program and adjustment policies.

The goals of this Privacy Program are to insure the security and confidentiality of consumer information, 16 CFR § 314.3(b)(1); protect the business against any anticipated threats or hazards to the security or integrity of consumer information, 16 CFR § 314.3(b)(2); and protect the business against unauthorized access to or use of consumer information that may result in substantial harm or inconvenience to a consumer, 16 CFR § 314.3(b)(3).

Designation of a Privacy Officer
This business does not maintain the position of Privacy Officer as a separate position.

Risk Assessment

Sources of Nonpublic Personal Information

Your business obtains personal nonpublic information individual purchasers of products and services (hereinafter "consumers"). The types of information received by about consumers include names, addresses, social security numbers, government issued identification (ex: driver's license), bank account information, credit reports, credit card numbers, and utility account numbers. This information is obtained from consumers who conduct transactions with this business.

Employee Training

Your business must provide training to new and existing employees about the need to keep and maintain all nonpublic personal information they may obtain secure. The employee training includes all applicable requirements of federal and state laws and regulations and this business' policies. The training also includes how to answer consumer's questions about how this business protects and safeguards nonpublic personal information. Information Systems

If this business maintains a network that allows employees to access electronically stored information, access is limited to an employee's need for the information to complete their job function or duty. Electronically stored nonpublic personal information includes:

- Completed High Dollar Transaction Forms
- Copies of consumer identification documents relating to the purchase of money orders and the completed High Dollar Transaction Forms
- Suspicious Activity Reports
- Copies of money orders supporting filed Suspicious Activity Reports
- Copies of money orders obtained to resolve problems a consumer may have relative to purchase and use of money orders
- Documents containing account information relating to the payment of utility or other bills by this business on behalf of FirsTech, Inc.
- Information Safeguards

This business obtains personal nonpublic information individual purchasers of products and services (hereinafter "consumers"). The types of information received by about consumers include names, addresses, social security numbers, government issued identification (ex: driver's license), bank account information, credit reports, credit card numbers, and utility account numbers. This information is obtained from consumers who conduct transactions with this business.

All employees provided nonpublic personal information by consumers about themselves to pay a fee associated with a product or service are prohibited from copying or retaining any nonpublic personal information. Employees receiving nonpublic personal information from consumers to pay for services shall place any document containing such information in a secure location until the required recordkeeping time period has passed. Employees may obtain copies of documents containing nonpublic personal information about consumers as part of their daily operations.

Some employees have access to a consumer's nonpublic personal information to perform his/her job functions. Any employee with access to a consumer's nonpublic personal information is strictly prohibited from copying, transcribing or otherwise duplicating that information for a purpose unrelated to their particular job function or duties. Any nonpublic personal information an employee copies, transcribes or otherwise duplicates to perform his/her job functions or duties must destroy or shred such copied, transcribed, or otherwise duplicated information immediately after completing the job function or duty requiring the nonpublic personal information.

Evaluation, Testing and Adjustments to Privacy Program
This business will perform periodic evaluations of this Privacy Program. Upon receipt of the results of the evaluation, the Privacy Officer will address any recommendations made by the auditor.

Exhibit A

PRIVACY POLICY: This business does not disclose any nonpublic personal information about walk-in bill pay consumers to any company, person, or individual except to FirsTech, or as otherwise required by law. This business restricts access to nonpublic personal information to those who need to know the information to facilitate the bill payment or for any other lawful purpose. This business maintains information safeguards that comply with all federal laws and regulations relating to the protection of nonpublic personal information.

Section V
Suspicious Activity Reporting

Suspicious Activity Reporting Requirements
The federal government requires an MSB to file a Suspicious Activity Report by Money Services Business (SAR-MSB) for any transaction – or pattern of transactions – that is attempted or conducted with at least $2,000, that a business knows, suspects or has reason to suspect:

- Involves funds derived from illegal activity or is intended to hide funds derived from illegal activity

- Is structured to avoid recordkeeping or reporting requirements; Has no business or apparent lawful purpose; or Facilitates criminal activity

- A SAR-MSB may be filed on suspicious activity below $2,000, but regulations do not require it

Filing Requirements for SAR-MSBs

A SAR-MSB must be filed within 30 days of detection of the suspicious event. The SARMSB must be filed online at;
http://bsaefiling.fincen.treas.gov/main.html

Recordkeeping for SAR-MSBs A copy of a SAR-MSB must be kept for at least five (5) years.

Section VI Currency Transaction Reporting

Currency Transaction Reporting Requirements
A Currency Transaction Report (CTR) must be filed with the federal government for any cash transaction that is greater than $10,000 conducted in one day, by any person, or on behalf of another person. The $10,000 threshold includes both the face amount of the transaction and all fees paid by the customer.

Filing Requirements for CTRs
A CTR must be filed within 15 days of the transaction. The CTR forms may be filed online at: http://bsaefiling.fincen.treas.gov/main.html
Recordkeeping for CTRs- A copy of each CTR must be kept for at least five (5) years

Section VII
Forms
Designation of a Compliance Officer
Employee Anti-Money Laundering Training
Designation of a Privacy Officer