Anti-Money Laundering

How to set up a **strong Compliance Program**

OnCourse Learning
FINANCIAL SERVICES

Importance of AML Protection

Financial institutions face a growing number of threats from criminals that seek to misuse the U.S. financial system. Cybercriminals are hacking into bank accounts, terrorists try to use the financial system to fund future attacks, and there are numerous money laundering issues.

As the use of financial technology increases, including mobile apps, people have the ability to send and receive money and data quickly online and support new types of currency.

Using this technology is called **FinTech.** FinTech has represented—and continues to represent—great challenges and opportunities for financial institutions.

As the first line of defense, you play an important role in protecting your institution by implementing an effective BSA/AML compliance program.

Money Services Defined

Financial institutions are required to assist the US government in the detection and prevention of money laundering.

More than 25% of US-based households use financial institutions or money transmitters for their financial needs, including sending money to family members located abroad.

They include:

Wealth management

Alternative finance

Payment platforms

Retail banking

Markets and exchanges

But anyone involved in transmitting money as a money services business (MSB) may fall under this definition. Let's take a closer look.

Compliance with government requirements has become more complicated due to the use of FinTech – technology used in financial transactions.

Broader Definition

AML regulations apply to any person doing business, whether or not on a regular basis or as an organized business concern, in the following capacities:

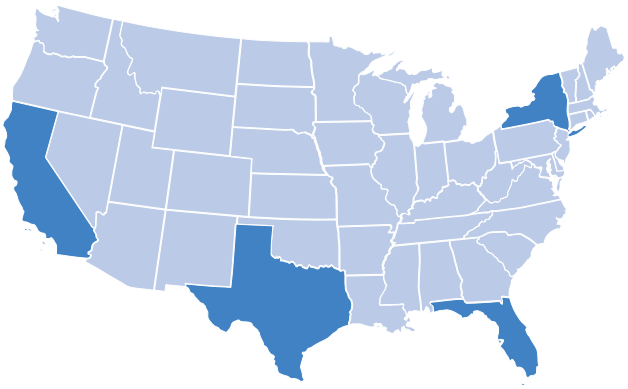
- Currency dealer or exchanger
- Check casher
- Issuer of traveler's checks, money orders or stored value
- Seller or redeemer of traveler's checks, money orders or stored value
- Money transmitter
- US Postal Service

It includes an activity threshold of greater than $1,000 per person per day in one or more transactions. No activity threshold applies to the definition of money transmitter.

If you fall into any of these categories, important federal and state requirements must be followed under FinCEN's AML requirements.

According to FinCEN,
in addition to the many MSBs that are **registered,**
there are thousands that are **unregistered.**

In 2011, depository institutions
submitted approximately **5,300** SARs
related to potential unlicensed activity.



Almost half were filed in
California, New York,
Texas, and Florida.

Of those submitted, many were
grocery stores, gas stations, or **liquor stores,**
operating as an MSB in some way.

The Registration Gap

Federal and State Requirements

FinCEN's AML requirements include:

- **Registration** with FinCEN
- Establishment of a **written compliance program** reasonably designed to prevent or facilitate money laundering or the financing of terrorist activities
- **Keeping records** and file reports to FinCEN related to suspicious activities
- Meeting specific **state requirements** for licensing criteria for certain types of MSBs, such as check cashing agencies and money transmitters

Note: fund transfers below $3,000 can occur without verification or recording of a consumers identification

Due to the emergence of FinTechs, meeting these requirements has grown in complexity as well as risk. Non-compliance can cause lawsuits and penalties. It also opens up the door for "bad actors" to exploit services.

Enforcement/Penalty Examples

If an MSB knows, suspects or has reason to suspect that a transaction or pattern of transactions is suspicious and involves $2,000 or more, the MSB must file a SAR.

Failure to report suspicious activity may lead to monetary penalties.

Ripple Labs

- Virtual currency XRP
- Operated the MSB without registering with FinCEN
- Failed to implement an adequate AML program and report suspicious activity

Ripple began dealing digital currency in 2013, but did not fully implement its AML compliance program for almost a year following commencement of sales. FinCEN assessed a $700,000 civil monetary penalty concurrent with the US attorneys office for the Northern District for CA's settlement agreement. It also included a forfeiture of $450,000.

Liberty Reserve

- "Susceptible" to being used for criminal activity
- Marketed as private
- Credentials were provided, but false credential were accepted

Users were able to convert their cash into digital currency, then back to cash. Transactions were anonymous and untraceable. According to the DOJ, many transactions were used to hide the proceeds of credit card theft, identity fraud, hacking and Ponzi schemes. The founder was sentenced to 20 years in prison, ordered to pay a $500,000 fine and forfeit $122 million in company profit.

The Essential Need for a Compliance Program

The best path to minimizing risk is establishing a robust compliance program. Building a program uncovers risks and enables you to mitigate them to an acceptable level.

Start by Assessing Risks

Identify your type of business

Products or services?

Define your customer base

What is the purpose of accounts and use of accounts?

Analyze geographic locations

Do they include high Intensity Drug Trafficking Areas (HIDTA) or high Intensity Financial Crime Areas (HIFCA)

Review your high risk factors

Are employee's trained on the BSA/AML regulations?

Are internal policies and procedures in place? Do you have a designated compliance officer?

Define Your Program

Once you outline your risk, the next step is developing a written program that defines a system of internal controls, how independent testing will be handled and who will be responsible for day-to-day management. A critical step is setting up training for your organization.

Ongoing due diligence is key. No anonymous payments.

Identify suspicious activity and a scalable process for SAR completions when necessary.

Make and retain records for any fund transmissions amounting to $3,000 or more.[9]

Your program should include the new customer due diligence procedure starting in May 2018.

A process needs to be defined for finding out the identity of the natural persons behind the legal entity customers – the beneficial owners.[8]

Develop **Five** Critical Internal Controls

1. Identify higher-risk banking operations
2. Inform key stakeholders of compliance initiatives, identified deficiencies, SARs filed and corrective action taken
3. Provide for program continuity despite changes in management, organization structure or staffing
4. Meet all regulatory requirements and plan for timely updates to implement changes in regulations
5. Train employees to be aware of their responsibilities under the BSA regulations and internal policy guidelines[10]

BSA/AML Officer

Designate a person or team responsible for the overall BSA/AML compliance program

- Determine whether the compliance officer has the necessary authority and resources to effectively execute all duties
- Assess the competency of the compliance officer and his or her staff, as necessary
- Analyze whether the compliance group is sufficiently staffed for the bank's overall risk level, size, and compliance needs
- Ensure no conflict of interest exists
- Provide staff adequate time to execute all duties[9]

Set Up Independent Testing

To protect your organization, 3rd party objective testing plays a critical role. It should include the following:

- A risk assessment and review of reporting and recordkeeping requirements
- CIP implementation
- Monitoring of the adequacy of CDD policies, procedures, and processes and whether they comply with internal requirements
- Reviewing personnel adherence to the bank's BSA/AML policies, procedures, and processes
- Testing transactions with particular emphasis on higher-risk operation (products, services, customers, and geographic locations)
- Assessment of training, including its comprehensiveness, accuracy of materials, the training schedule and attendance tracking
- Verification of deficiencies correction
- Reviewing policies, procedures and processes for suspicious activity monitoring
- Evaluation of the system's methodology for establishing and applying expected activity or filtering criteria
- Assessing the system's ability to generate monitoring reports[10]

Create a Training Program

A formal training program makes a statement about the importance the board of directors and senior management places on ongoing education, training, and compliance. It also ensures employee accountability for ensuring compliance.

A comprehensive approach considers the specific risks of individual business lines, including:

- Documentation of attendance records and training materials
- Coverage of bank policies, procedures, processes and new rules and regulations
- Coverage of different forms of money laundering and terrorist financing as it relates to identification and examples of suspicious activity
- Penalties for noncompliance with internal policies and regulatory requirements[10]

By taking these steps, from **assessment** to **training**, you'll create a strong layer of defense against financial predators as well as ensure compliance with the law.

Are you compliant?

A strong compliance program offers the best line of defense to protect your company, consumers and your reputation.

Build a compliance program with these five basic pillars for success:

1. Designate a compliance officer
2. Create internal policies, procedures and controls
3. Provide ongoing, relevant employee training
4. Independent review of policies and procedures
5. Conduct ongoing customer due diligence

Remember, prevention beats the cost and time of remediation.

Ready to get started?

Visit **OnCourseLearning.com/Business** for more information.

References

1. www.irs.gov/businesses/small-businesses-self-employed/money-services-business-msb-information-center

2. 31 U.S. Code § 5330 (d) (1)

3. www.irs.gov/uac/newsroom/irs-virtual-currency-guidance

4. www.marketwatch.com/story/occs-Fintech-charter-plan-draws-debate-2017-06-23

5. www.jdsupra.com/legalnews/csbs-sues-occ-over-Fintech-charters-14261/

6. www.crowdfundinsider.com/2017/05/100462-csbs-vision-2020-answer-occ-Fintech-charter/

7. www.financialservicesperspectives.com/2016/07/the-fifth-pillar-of-amlbsa-compliance-fincen-issues-final-rule-for-new-customer-due-diligence-requirements-under-the-bank-secrecy-act/

8. www.mondaq.com/unitedstates/x/524446/fin+tech/Complying+With+AML+Laws+Challenges+for+the+Fintech+Industry

9. www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_008.htm