ANTI-MONEY LAUNDERING

How to Setup a Strong Compliance Program

Banks • Credit Unions • Mortgage • Non-Bank Financial Institutions

OnCourse Learning

Overview

Financial institutions face a growing number of threats from criminals that seek to misuse the U.S. financial system. Cybercriminals are not only hacking into bank accounts, but in this age of remote work, are also trying to gain access to financial institution systems.

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

TABLE OF CONTENTS

What to Expect

In this ebook you will learn the importance of anti-money laundering (AML) protection and how an effective compliance training program is key to your institution's success.

Use of Technology: **Fintech**

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

Fintech has represented - and continues to represent - great challenges and opportunities for financial institutions.

Compliance with government requirements has become more complicated due to the use of Fintech.
Read more on federal and state requirements on **page 6**.

MONEY SERVICES

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

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

INCLUDE:

Wealth Management

Alternative Finance

Payment Platforms

Retail Banking

Markets & Exchanges

Anyone involved in transmitting money as a money services business (MSB) may fall under this definition.

Source:
2017 - FDIC National Survey of Unbanked and Underbanked Households - Executive Summary

BROADER DEFINITION

of AML Regulations

Anti-money laundering (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
- U.S. 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.

THE REGISTRATION GAP

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

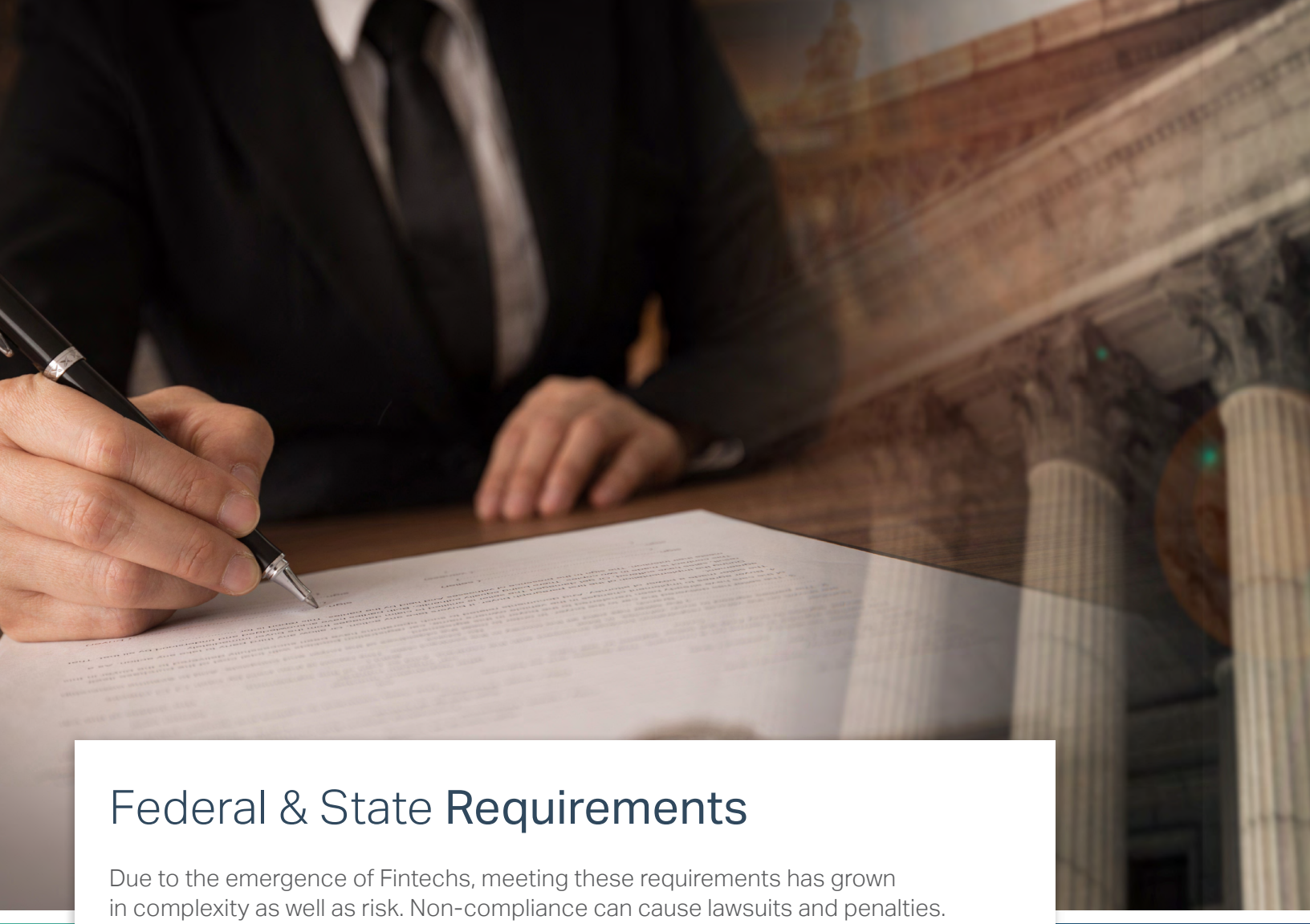
4,700

In 2019, depository institutions submitted approximately **4,700 SARs** related to potential unlicensed activity.

47%

47% were filed in California, Colorado, Florida, New York and Texas.

Of those submitted, many were **grocery stores, gas stations, or liquor stores**, operating as a money service business (MSB) in some way.



Federal & State **Requirements**

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. **Fund transfers below $3,000 can occur without verification or recording of a consumer's identification.**

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

Source:
Guidance on Existing AML Program Rule Compliance Obligations for MSB Principals with Respect to Agent Monitoring

Enforcement/Penalty **Examples**

If a money service business (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 Suspicious Activity Report (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 anti-money laundering (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 U.S. attorney's office for the Northern District for CA's settlement agreement. It also included a forfeiture of $450,000.

Source:
FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger

LIBERTY RESERVE

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

Source:
Liberty Reserve Founder Sentenced to 20 Years For Laundering Hundreds of Millions of Dollars

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.

- Designate a compliance officer
- Create internal policies, procedures and controls
- Provide ongoing, relevant employee training
- Independent review of policies and procedures
- Conduct ongoing customer due diligence

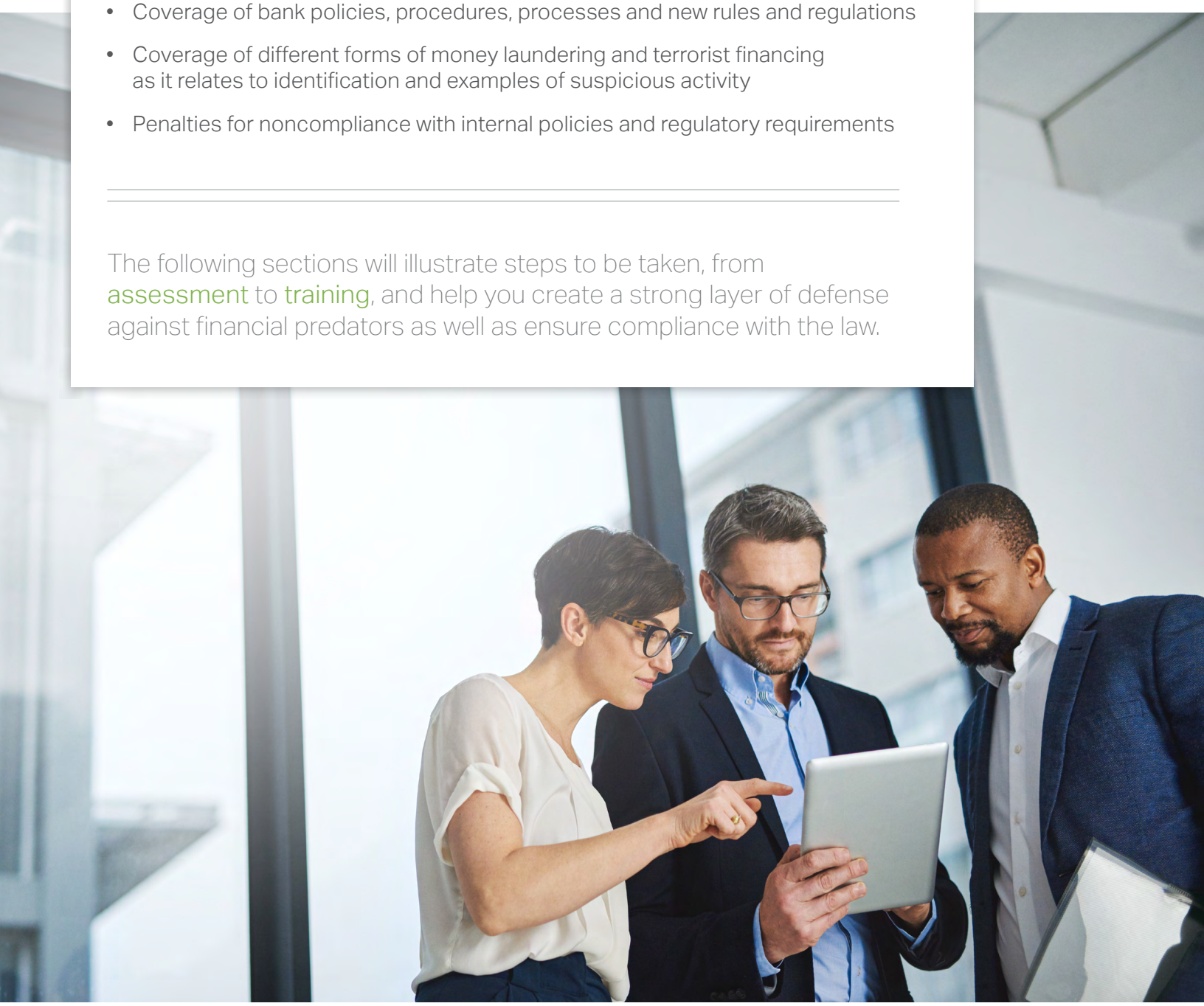
Create a **Training Program**

A formal training program makes a statement about the importance of 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

The following sections will illustrate steps to be taken, from assessment to training, and help you create a strong layer of defense against financial predators as well as ensure compliance with the law.



01 ASSESS 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 employees trained on the BSA/AML regulations? Are internal policies and procedures in place? Do you have a designated compliance officer?

02 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

  No anonymous payments

- Identify Suspicious Activity

  Identify suspicious activity and scalable process for SAR completions when necessary

- Make and Retain Records

  Make and retain records for any funds transmissions amounting to $3,000 or more

---

Your program needs to include the Customer Due Diligence Rule (CDD).

CDD has 4 core requirements:

- Identify and verify the identity of customers
- Identify and verify the identity of the beneficial owners of companies opening accounts
- Understand the nature and purpose of customer relationships to develop customer risk profiles
- Conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, maintain and update customer information

03 DEVELOP INTERNAL CONTROLS

- Identify Higher-Risk Banking Operations
- Inform Key Stakeholders

  Inform key stakeholders of compliance initiatives, identified deficiencies, SARs filed and corrective action taken

- Provide for Program Continuity

  Provide for program continuity despite changes in management, organization structure or staffing

- Meet All Regulatory Requirements

  Meet all regulatory requirements and plan for timely updates to implement changes in regulations

- Train Employees

  Train employees to be aware of their responsibilities under the BSA regulations and internal policy guidelines

Source:
Information on Complying with the Customer Due Diligence (CDD) Final Rule

04 DESIGNATE COMPLIANCE OFFICERS

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

- **Determine** Authority

  Determine whether the compliance officer has the necessary authority and resources to effectively execute all duties

- **Assess** Competency

  Assess the competency of the compliance officer and his or her staff, as necessary

- **Analyze** Compliance Group

  Analyze whether the compliance group is sufficiently staffed for the bank's overall risk level, size and compliance needs

- **Ensure** No Conflict

  Ensure no conflict of interest exists

- **Provide** Staff Time

  Provide staff adequate time to execute all duties

05 SETUP INDEPENDENT TESTING

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

- Risk Assessment and Review

  A risk assessment and review of reporting and recordkeeping requirements

- CIP Implementation

- Monitor Policies, Procedures and Processes

  Monitoring of the adequacy of CDD policies, procedures, and processes and whether they comply with internal requirements

- Review Personnel Adherence

  Reviewing personnel adherence to the financial institution's BSA/AML policies, procedures and processes

- Test Transactions

  Testing transactions with particular emphasis on higher-risk operation (products, services, customers and geographic locations)

- Assess Training

  Assessment of training, including its comprehensiveness, accuracy of materials, the training schedule and attendance tracking

- Verification of Deficiencies Correction

- Review Suspicious Activity Monitoring

  Reviewing policies, procedures and processes for suspicious activity monitoring

- Evaluate Filtering Criteria

  Evaluation of the system's methodology for establishing and applying expected activity or filtering criteria

- Monitor Reports

  Assessing the system's ability to generate monitoring reports

Ready *to*

LEARN MORE?

OnCourse Learning provides a comprehensive solution for your compliance training and personal development.

Request a demo at OnCourseLearning.com

OnCourse Learning is a member of the Adtalem Global Education Financial Services Workforce Solutions family which includes: the Association of Certified Anti-Money Laundering Specialists (ACAMS), its CAMS certification is one of the most widely recognized anti-money laundering certifications among compliance professionals worldwide; Becker Professional Education, which offers programs in CPA Exam Review and continuing professional education courses; and EduPristine, one of India's leading training providers in accounting, finance and digital marketing.

OnCourse Learning

CONTACT US

Contact OnCourse Learning for more information.

(866) 806 - 9900

www.OnCourseLearning.com