BEST PRACTICES FOR US MONEY SERVICES BUSINESSES

Anti-Money Laundering and Counter-Financing of Terrorism Compliance Program

May 11, 2022

Acknowledgements

The Electronic Transactions Association ("ETA"), INFiN—a Financial Services Alliance, the Money Services Business Association ("MSBA"), and The Money Services Round Table ("TMSRT") wish to acknowledge the regulatory and law enforcement agencies, financial institutions, money services businesses, trade organizations, banks, public policy bodies, and numerous individuals that provided feedback on this document and help the industry-driven effort to improve compliance with AML/CFT regulations. Consultations among Bank Secrecy Act Advisory Group ("BSAAG") members were instrumental and informed the development of these industry Best Practices through cross-sector discussions.

Notable individual contributors and editors include, but are not limited to:

Duncan DeVille; Wm. Clay Roberts; Diego Rosero; Paul Dwyer; Joseph Mignano; Joseph (Jody) Myers; Elizabeth Cronan; Robert Rowe; Alan Abel; J.R. Davis; Andres Villareal; and Reno Mathews.

Statement of Purpose

This Best Practices guide is designed to assist Money Services Businesses ("MSBs") with developing a compliance program to meet applicable requirements established by the Financial Crimes Enforcement Network ("FinCEN"), its implementing regulations under 31 CFR § 1022, FinCEN's *Bank Secrecy Act ("BSA")/Anti-Money Laundering ("AML") Examination Manual Money Services Businesses,* sanctions laws/regulations, and relevant guidance. Like the underlying laws, these best practices are not designed to be a "one-size-fits-all" solution to complying with regulations, but should be implemented on a risk-basis commensurate to the size of the MSB, the services it offers, the geographies in which it operates, and other pertinent factors. The practices discussed in this document were formulated as best-in-industry principles to assist any MSB in meeting its regulatory obligations. To this end, these best practices also take into account virtual currency and financial-technology "FinTech" companies recognizing their integration into the financial services landscape and accompanying AML obligations.

In addition to assisting with general regulatory requirements, banks and other financial institutions will be encouraged to confidently engage in relationships with MSBs that utilize these standards and best practices. Further, banks and other financial institutions can utilize these best practices to address the regulatory expectations described in the *FFIEC BSA/AML Examination Manual.* These expectations include:

- That "[t]he BSA does not require, and neither FinCEN nor the federal banking agencies expect, banks to serve as the *defacto* regulator" of any Money Services Business;[1]
- That "[w]hile banks are expected to manage risk associated with all accounts, including MSB accounts, banks will not be held responsible for the MSB's BSA/AML program;"[2] and
- That "[n]ot all MSBs pose the same level of risk, and not all MSBs will require the same level of due diligence. Accordingly, if a bank's assessment of the risks of a particular MSB relationship indicates a lower risk of money laundering or other illicit activity, a bank is not routinely expected to perform further due diligence (such as reviewing information about an MSB's BSA/AML program) beyond the minimum due diligence expectations. Unless indicated by the risk assessment of the MSB, banks are not expected to routinely review an MSB's BSA/AML program."[3]

As described in this best practices document, an MSB should address its AML risk in accordance with relevant government regulation and the risk posed by its own business model. MSBs are diverse entities engaging in many types of commerce, including dealers in foreign exchange, check cashers, sellers of prepaid access, providers of prepaid access, issuers or sellers of traveler's checks or money orders, and money transmitters. However, the principles described in this best practices document can guide the implementation of an AML

[1] FFIEC Bank Secrecy Act Anti-Money Laundering Examination Manual, Risks Associated with Money Laundering and Terrorist Financing, Non-Bank Financial Institutions - Overview.

[2] Ibid.

[3] Ibid.

program for any MSB involved in any activity regardless of the MSB's services, size, or geographic reach. Overall, these industry best practices should enable an MSB to develop and maintain an AML program to meet its obligation to detect, report, and prevent money laundering and terrorist financing. This best practices document is not intended to be exhaustive and MSBs should review the materials cited herein and comply with all applicable laws and regulations.

Table of Contents

Chapter I
A Primer on Money Services Businesses

1. Defining MSBs, their Products and Limits

MSBs are categorized as Non-Bank Financial Institutions ("NBFIs"), which are broadly defined as financial institutions other than banks that offer financial services. Other common examples of NBFIs include operators of credit card systems, investment advisers, mutual funds, insurance companies, loan, or finance companies, etc.

Further defining MSBs, FinCEN, the bureau within the US Department of the Treasury that administers the federal anti-money laundering laws known as the Bank Secrecy Act ("BSA"), defines MSBs as persons doing business in one or more of the following capacities: [4]

- Issuer or seller of traveler's checks or money orders;
- Money transmitter;
- Dealer in foreign exchange;
- Provider of prepaid access;
- Seller of prepaid access;
- US Postal Service; and
- Check casher.

As exemplified above, the definition of MSBs is in part based on the products and services this type of financial institution offers. For example, FinCEN clarified in 2013 that certain exchangers of virtual currency, based on the services they offer, are MSBs.[5] MSB products and services in turn shape the type of relationship that MSBs have with their consumers. Unlike banks, MSB products and services are not necessarily account based.

MSBs, like other financial institutions such as banks, must develop and implement Anti-Money Laundering ("AML") programs as required by the BSA, which should be tailored to address and mitigate the risk surrounding the products, geographic footprint, and consumer base serviced.[6]

Because MSBs range from larger, global companies to smaller businesses, they may offer a wide variety of products and services carrying varying degrees of risk. Therefore, MSBs should create an inventory of all products its business will offer, identify the AML risks associated with such products, and then place reasonable, risk-based controls on each one. Those limits may restrict, for example, the frequency, dollar amount, or jurisdictions where the product may be offered.

Therefore, determining where it would operate and the products it may offer, must be one of the – if not the – first steps taken in establishing the type of business an MSB wishes to be.

---

[4] *See* 31 CFR § 1010.100(ff).

[5] *See* FinCEN guidance FIN-2013-G001 "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies" (March, 2013).

[6] See generally 31 CFR §§ 1022.200 and 1022.210.

Chapter Resources:

- Definition of an MSB:
  - Definition published by FinCEN (https://www.fincen.gov/money-services-business-definition).
  - 31 CFR § 1010.100(ff) (https://www.ecfr.gov/cgi-bin/text-idx?SID=b0df8afef7a2cbedffe549bdc28c3d66&mc=true&node=se31.3.1010_1100&rgn=div8).
- Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies:
  - FinCEN guidance FIN-2013-G001 (March, 2013) (Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies).
- AML Program requirements for MSBs:
  - 31 CFR §§ 1022.200 and 1022.210 (https://www.ecfr.gov/cgi-bin/text-idx?SID=9fff79cd694f8b9d0050e7f5f7453978&mc=true&node=pt31.3.1022&rgn=div5#sp31.3.1022.b).

Chapter II
Building an Effective AML Program

1. Overview

MSBs, through their respective AML programs, play a key role in safeguarding the financial system from illicit use, including money laundering, terrorist financing, and other illicit activities. To this end, FinCEN has issued regulations requiring MSBs to implement an appropriate risk-based AML program designed to effectively address their specific money laundering and terrorist financing risks.[7]

The overarching goals of implementing an effective AML program are to:

- Prevent the MSB from being used to facilitate money laundering and terrorist financing; and
- Meet the requirements of the BSA.

Regardless of the size, structure, consumers, services, or complexity of an MSB, the elements of an AML program remain the same. The implementation of the AML program will be dependent on the type of the MSB and the nature of its business footprint.

MSBs are required to document their AML programs in writing, which should incorporate the below four "pillars," or components, which reinforce and build upon one another:

- Designation of a qualified BSA/AML officer;
- Establishing policies, procedures, and controls;
- Training; and
- Independent audit/testing.

It is important to note that banks that provide services to MSBs may, as part of knowing their customers, request to see, among other things, an MSB's written compliance program, policies and

[7] *See* 31 CFR §§ 1022.200 and 1022.210.

procedures, and AML risk assessment. While MSBs are not required to provide such documentation to their partner banks, MSBs should work closely with them to identify the documentation and information that would help secure and maintain the financial relationship.

2. AML Risk Assessment

An AML program should be based on an ongoing, business-specific risk assessment. It is the roadmap that will inform the AML program and all other product, service, control, and process decisions AML management makes. The risk assessment is the tool used to identify the nature and extent of AML risks so that the AML program includes tailored and effective risk mitigating measures. The risk assessment may be formal or informal, but preferably documented. MSBs, however, should be prepared to justify informal risk assessments, which may be appropriate for less complex companies.

Risk assessments should take into account an MSB's consumer base, geographic footprint, and services offered. For example: small money transmitters servicing single corridors (e.g., money transfers originating and being paid only within a single state) may need to focus AML risk assessments on consumers served within the corridor and the nature of the transactions provided; for medium-sized check cashers, the risk assessment may focus on the likelihood of fraudulent checks and on identifying consumers and their respective activities; for large prepaid access providers, the risk assessment may involve an in-depth evaluation of the distribution channels for the prepaid access, evaluation of consumer usage, and determination of payment locations, among other factors.

A. Assessing AML Risk

MSBs should assess their ML/FT risks to ensure that their AML programs are focused on mitigating risk and that their leadership is informed and able to make risk-based decisions about business investments and risk mitigation.

i. Scope and Complexity of Coverage

Risk assessments should identify and address both the criminal environment (market threat) that is relevant to the MSB's business operations as well as the vulnerability of the business to abuse by criminals; consideration should also be given to assessing the consequences associated with various risks. In the first instance, risk assessments should focus on real risks, i.e., the potential for abuse of the business by criminals. Regulatory, reputational, and enforcement risks, i.e., the potential for adverse impact arising from the materialization of real risk, can also be considered but should be distinguished from real risk. The depth and complexity of analysis of an MSB's risk should be proportionate to the size, scope, and complexity of the MSB's business. Larger and more complex businesses may assess and document risk at multiple levels of their operations.

Assessment of market threats should consider known typologies that affect the risk as well as potential emerging threats. Assessment of vulnerability should address inherent structural aspects of the MSB's business that affect the risk (e.g., consumers, products and services, means of delivery of services, geographic locations, etc.) as well as the existence and effectiveness of controls that are currently in place to mitigate the risk. Risk assessments should evaluate risk and vulnerability both as an inherent matter (prior to the application of controls), and as a residual matter, after considering the effectiveness of controls in place. Risk assessments should also identify potential areas where strengthened controls could further mitigate risk, and – where possible – suggest specific control improvements.

ii. Methodology

Risk assessments should be based on both quantitative and qualitative information, from both internal and external sources. Criminal threat information may be found in government reports and other published sources, as well as derived from formal and informal interactions between the MSB and law enforcement and regulatory authorities. Vulnerability information can include business records, surveys, and interviews with the MSB's business, operations, and compliance personnel, as well as information from external sources such as regulatory bodies, independent auditors and consultants, international bodies such as the Financial Action Task Force ("FATF"), and even information provided by consumers. Information should be compiled into a structured analysis designed to clarify and differentiate the underlying drivers of risk, and to isolate areas where improved controls can mitigate risk. Risk elements should be scored and arrayed across a matrix to identify higher, medium, and lower risk exposure.

iii. Governance and Follow-Up

Risk assessments should be reviewed and approved by appropriate management, including the Board of Directors ("Board") or a Board committee as necessary, of the MSB. Recommendations for potential improvements in controls should be similarly considered and addressed, either through follow-up or through risk acceptance decisions by appropriate leadership (i.e., a decision by the business line to accept certain risk). MSBs should document various elements of the risk assessment process, including: the assessment methodology; working papers and the underlying basis for reaching conclusions; summaries of results used to communicate to business leaders, staff, and regulators; and identified areas for potential to strengthen controls; and risk acceptance decisions.

iv. Ongoing Updates

Risk assessments should be updated periodically to reflect material changes in the products offered, customer base, and geographies as well as the inherent risk and the control environment of these factors. The frequency of updates may be a function of the level of risk identified in previous assessments, as well as the degree of change in the risk environment during the intervening period. Evolving factors such as products offered, geographic risk, geopolitical events, and economic conditions may affect the frequency with which an MSB conducts its risk assessment. As a best practice, MSBs may conduct their formalized review periodically (e.g., annually) but adjust risk mitigating controls as necessary to address new or previously unknown AML risks.

As part of these updates, MSBs should also consider the effectiveness of any newly implemented risk mitigating measures as well as changes in legislation and shifts in the regulatory landscape (including enforcement actions taken by regulatory agencies).

3. AML Program "Pillars"

The observations resulting from the risk assessment should inform and guide the MSB's development and implementation of its AML program. In doing so, the MSB's AML program should include measures to support the below program components, or "pillars."[8]

[8] FinCEN's 2015 and 2017 enforcement actions against Ripple Labs Inc. and BTC-e exemplify how failing to establish an effective AML program can open MSBs to money laundering threats and regulatory violations.

BEST PRACTICES FOR US MSBs: AML & CFT COMPLIANCE PROGRAMS

A. BSA/AML Compliance Officer and Staffing

Ultimate responsibility for an MSB's AML compliance resides with its most senior leadership, such as the Board. Owners, Boards, or representatives of senior management must appoint BSA/AML officers to oversee the MSB's day-to-day compliance. This designation is typically memorialized in Board meeting minutes, and notification of such designation to regulatory agencies may be required. Simply naming someone to this role is not enough. The BSA/AML Officer is ideally an individual who:

- Demonstrates certain minimum qualifications, which may even be prescribed by state regulations, such as expertise in BSA/AML regulations and professional experience, which may include recognized industry certifications and degrees;
- Has the capacity to coordinate, manage, and oversee day-to-day compliancewith the BSA and its implementing regulations;
- Is empowered and has the appropriate level of authority, responsibility, and access to resources within the MSB, such as an appropriate budget and staffing;
- Understands how to implement appropriate risk mitigating controls for the company's product and service offerings, consumer base, and associated risks;
- Has the ability to influence the MSB's business teams and decisions;
- Communicates with regulators and fellow Compliance Officers and attends industry outreach events;
- Can confidently engage in discussions with examiners and auditors on the details of the MSB's AML program;
- Regularly informs the Board and senior management of AML compliance initiatives, potential issues, audit and examination report observations, and corrective actions;
- Has an independent reporting line in the company and her/his compensation structure does not create any conflicts of interest;
- Has ongoing support from senior management that ensures compliance efforts and her/his compensation are not negatively impacted by company profits or revenue interests (this would enable independent risk-based decisions); and
- Has a line of communication or is able to provide information to the Board orother executives.[9]

As an example of different scenarios, for medium sized providers of prepaid access, the BSA/AML Compliance Officer may also have other duties in addition to overseeing a compliance team focused on BSA/AML matters. For a larger money transmitter, the BSA/AML Compliance Officer may oversee a sizable team focused on BSA/AML matters. In all cases, the BSA/AML Compliance Officer should be able to dedicate the adequate time to oversee the program and should be of sufficient seniority to effect change within the organization.

[9] See generally, FinCEN's 2014 advisory on "Promoting a Culture of Compliance" which indicates that "[c]ompliance staff should be empowered with sufficient authority and autonomy to implement an institution's AML program. An institution's interest in revenue should not compromise efforts to effectively manage and mitigate BSA/AML deficiencies and risks, including submission of appropriate and accurate reports to FinCEN."

B. Internal Controls

A system, or structure, of internal controls must be in place at each MSB. That system, based on the results of an ongoing risk assessment, creates the framework for an effective compliance program. As applicable, MSBs should consider developing internal control processes for:

- Appropriate involvement of the MSB's business line in risk management decisions and controls;
- Policies and procedures, including periodic reviews and updates;
- Consumer identification;
- Integrating automated data processing of attempted and completed transactions;
- Monitoring to identify reportable activity and transactions;
- Tools calibrated to the specific MSB model;
- Dual control and segregation of duties;
- Management information reporting;
- Regulatory reporting, including quality assurance and/or control processes;
- Responding to law enforcement and other information requests; and
- Recordkeeping and retention.

MSBs should keep in mind that regulators generally expect controls to be documented. It may not be enough to be able to verbally explain the control system or process without providing an accompanying procedure document against which examiners can test. It is also worth noting, the act of creating written procedures that do not reflect actual practices will also garner regulatory criticism.

C. AML Training

Documenting processes and requirements is an important step toward meeting requirements. The next logical step is to ensure all appropriate employees are trained to understand and adhere to these processes and requirements. As applicable, MSBs should consider:

- Requiring training for newly hired employees either before they begin working or within a very short period after commencing work;
- Requiring ongoing AML training for all employees regardless of role or title;
- Tailoring training content to job descriptions ensuring those with highest risk jobs receive more frequent and more targeted and detailed training;
- Updating training content to include changes in internal policies, regulations and lessons learned from recent enforcement actions;
- Ensuring that individuals who change jobs receive appropriate training within a reasonable period after assuming the new responsibilities;
- Providing access to specialized training and certifications for compliance officers and other staff, as appropriate;
- Creating Board and senior management specific training to convey the importance of a "culture of compliance" and to explain the contents of audit and examination reports that they will receive;
- Requiring ongoing/annual and relevant training rather than a one-time, one-size-

fits-all training;

- Evaluating comprehension after training sessions and retraining if employees fail to grasp concepts;
- Offering targeted training when employees breach specific internal or regulatory requirements;
- Issuing reminders to employees and supervisors of employees when training is coming due;
- Retaining records of all training materials and attendance logs; and
- Where appropriate, connecting training completion to employee performance, bonus, and reward systems.

While not required, MSBs may consider computerized training, which can offer many advantages, such as more accurate training records and scheduling flexibility.

D. Independent Testing

The fourth pillar of a sound compliance program is the independent, or third party, review of the other program pillars. While the risk assessment the MSB performs should dictate the frequency with which independent testing is performed, MSBs should generally consider having annual testing, at minimum. If hiring a third party to conduct independent testing, an MSB should consider the third party's level of expertise, staffing, methodology, and reputation among other factors in making its hiring selection.

Regarding independent testing, there are several important points for MSBs to consider, including:

- Regulators will assess the competency, independence, and any potential conflicts of interest of the third party selected to perform testing;
- The reviewer, or testing team, must be truly independent, which may include an Internal Audit department;
- MSBs should carefully retain qualified third-party firms – with expertise in the products and services particular to the MSB – to perform the independent review;
- MSBs should obtain and document Board/management selection and approval of the selected independent reviewer;
- Upon completion of the review, the final testing report should be addressed directly to the Board; and
- MSBs should consider new independent parties every few years to ensure a fresh perspective.

When vetting third party firms, MSBs should verify that the scope of the independent test includes:

- Review of the risk assessment;
- Transaction testing to verify adherence to reporting and recordkeeping;
- Review of monitoring systems;
- Review of sanctions monitoring systems, as appropriate;
- Testing of processes to identify unusual activity;
- Evaluation of adequacy of human and other resources;
- Determination of the adequacy of training materials and record retention;

- Assessment of management's efforts to remediate previously identified issues;
- Evaluation of the overall adequacy and effectiveness of the AML compliance program; and
- An executive summary and audit opinion.

When preparing for the independent testing process, MSBs should:

- Designate one or more knowledgeable point(s) of contact to interact with the auditors;
- Provide training to staff on the audit process, interacting with auditors, and the process for providing documents and answers to auditor questions;
- Track requests and retain records of all items provided;
- Request feedback throughout the review process as issues are identified and escalate material items to senior management immediately;
- Request that the auditors cite compliance and legal requirements for any identified issues when possible; and
- Following the review, develop specific action plans to resolve identified issues, assign ownership, and track findings through to resolution, since subsequent auditors will review remedial actions.

Consumer Due Diligence and Beneficial Ownership Rule (Not Applicable to MSBs)

While not applicable to MSBs, FinCEN's Customer Due Diligence Final Rule ("CDD"),[10] sometimes referred to as "the Fifth Pillar of AML Compliance," adds new obligations for covered institutions to understand the nature and purpose of customer relationships with the goal of developing customer risk profiles and, on a risk basis, maintain and update customer information, including information on the actual people (beneficial owners) of legal entity customers.

The CDD Rule does not currently apply to MSBs. However, with the potential that this requirement could pertain to MSBs in the future, it is worth considering its implications when building a compliance program and establishing due diligence policies and procedures.[11]

In addition, as detailed in Chapter IV, an MSB should perform appropriate due diligence on any prospective and current agents, including documenting agent ownership to a suggested minimum of 10% ownership level, or as required by regulation.[12]

4. Culture of Compliance (Line of Business Involvement)

While compliance personnel of MSBs are the individuals responsible for designing and

[10] On May 5, 2016, FinCEN issued a final rule imposing a requirement that certain financial institutions—but not MSBs—include in their AML programs risk-based customer due diligence procedures. The final rule became effective July 11, 2016 and required all covered institutions to comply by May 11, 2018.

[11] While many MSB operating models do not involve opening "accounts," if certain services (e.g., business to business payments, opening of accounts) are offered by an MSB, it is foreseeable that collection and verification of beneficial ownership could be required by FinCEN in the future; FinCEN has indicated it may extend CDD requirements to other financial institution types.

[12] Please refer to Chapter IV for further information on agent ownership due diligence.

implementing all pillars of a compliance program as described above, the success of the program depends on a strong companywide, senior level commitment to a culture of compliance. If the risk assessment is the framework upon which each pillar of a compliance program is built, a strong compliance culture is the insurance for the program.

In a 2014 Advisory,[13] FinCEN explains that MSBs will successfully create cultures of compliance if:

- The leadership team is active and engaged in understanding compliance efforts;
- The desire to increase revenue does not supersede mitigating risks;
- Information is shared across various departments; and
- Adequate resources are devoted to compliance initiatives.

Best practices across financial institutions, including MSBs, employ a three-lines-of- defense model, where risk is managed and mitigated across the business lines and operational management (first line), the enterprise-wide or corporate risk management and compliance functions (second line), and internal audit (third line). As applicable, MSBs should clarify sustainable roles and responsibilities across the three lines of defense commensurate with the complexity and risk of their business models. The lines of defense should be differentiated, with specific roles and responsibilities, clearly articulated in the appropriate policies and procedures of the organization.

In smaller organizations without an internal audit department, the MSB should have policies and procedures that provide for the review of critical areas by an independent internal resource (e.g., a manager that is not in charge of those critical areas).

In short, Compliance departments do not exist without the business lines and vice versa. With this in mind, an MSB compliance officer should:

- Define and communicate cultural values and expectations;
- Be involved in new product discussions with the business staff prior to launch;
- Thoughtfully consider ways to serve the consumers of the MSB without ever sacrificing necessary controls;
- Create frequent opportunities for Compliance and business representatives to discuss successes, opportunities, challenges, and ways to support each group's initiatives; and
- Provide safe ways for employees to report bad news quickly.

[13] *See* FinCEN advisory FIN-2014-A007: "Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance" (August, 2014).

Chapter Resources:

- AML Program requirements for MSBs:
  - 31 CFR §§ 1022.200 and 1022.210 (https://www.ecfr.gov/cgi-bin/text-idx?SID=9fff79cd694f8b9d0050e7f5f7453978&mc=true&node=pt31.3.1022&rgn=div5#sp31.3.1022.b).
- Customer Due Diligence Rule:
  - 31 CFR § 1010.230 "Beneficial ownership requirements for legal entity customers" (https://www.ecfr.gov/cgi-bin/text-idx?SID=54d4cd9f7a0e00ebe61750bfd0d9e00a&mc=true&node=se31.3.1010_1230&rgn=div8).
  - FinCEN's "Customer Due Diligence Requirements for Financial Institutions" Final Rule (https://www.gpo.gov/fdsys/pkg/FR-2016-05-11/pdf/2016-10567.pdf).
- Promoting a Culture of Compliance in Financial Institutions:
  - 2014 FinCEN advisory FIN-2014-A007 (https://www.fincen.gov/sites/default/files/shared/FIN-2014-A007.pdf).

Chapter III
Know Your Customer/Transactor

1. **Overview**
2. **Definitions**
3. **Standards for Information Collection**
4. **Defining Occasional Transactors and Regular Consumers with an Ongoing Business Relationship**
5. **Establishing Due Diligence and Enhanced Due Diligence Standards**
6. **Implementing Controls Based on Consumer Activity or Profile**

1. Overview

MSBs operate a variety of business models that may be categorized by two relationshiptypes: transaction-based relationships, and account-based relationships. These two relationship types may be further divided into subcategories: in-person transactions, non-in-person transactions, occasional transactions, and ongoing relationships (see illustrative chart below).

	Transaction-based relationships	**Account-based relationships**
In-person transactions	(e.g., cash-funded money transfers)	(e.g., cash-reloadable pre-paid access)
Non-in-person transactions	(e.g., bank account-funded money transfers/bill payments)	(e.g., virtual wallet moneytransfers)
Occasional transactions	(e.g., check cashing)	(e.g., virtual wallet moneytransfers)
Ongoing relationships	(e.g., reloadable pre-paid access)	(e.g., virtual wallet moneytransfers)

2. Definitions

Transactor – Any person directly obtaining products or services on his/her own behalf or on behalf of another.

3. Standards for Information Collection

MSBs collect consumer information for various business purposes, including to identify the consumers, transactors, receivers, or payees, as well as for regulatory purposes, such as compliance with the "Funds Recordkeeping" and "Travel" rules.[14, 15] In addition to using this information to facilitate payments, MSBs should use this information, as appropriate, to address fraud, sanctions screening, money laundering risks, and obligations to ensure consumer protection.

[14] *See* 31 CFR § 1010.410(e)-(f).

[15] On October 27, 2020, FinCEN proposed lowering the threshold for the Funds Recordkeeping and Travel rules from $3,000 to $250 for international transactions and for certain transactions involving convertible virtual currencies. MSBs should track any potential changes to the stemming from this notice of proposed rulemaking.

Based on its risk assessment and its business model, and even when not required by regulatory requirements, an MSB should consider collecting the following minimum information:

- The complete name of the transactor;
- The address of the transactor;
- The complete name of the recipient of the transaction; and
- An identification reference or number for the transaction.

MSBs should collect and review additional information based on the risk factors associated with the transaction, including:

- Contact information for the transactor;
- Contact information for the recipient;
- Identifying information for the transactor or recipient;[15]
- Occupation of the transactor and source of funds for the transaction;
- Purpose of the transaction; and
- Account numbers, if applicable.

4. Defining Occasional Transactors and Regular Consumers with an Ongoing Business Relationship

MSBs should independently determine if their business models target occasional transactions or account-based relationships. MSBs that engage in a transactional model are characterized by consumers that utilize the MSB on a "per transaction basis" and may or may not conduct repeat business with the MSB; whereas, MSBs that engage in an account model gather consumer information and establish a common account repeatedly used by the consumer.

In both models, a consumer could be an occasional or single use transactor or the consumer could use the services of the MSB on a regular basis. To have an effective monitoring program, an MSB must develop risk-based tools that are reasonably designed for its respective business model (see Chapter V). MSBs should be able to segment their client base according to the types of interactions with consumers.

Below are examples of actions MSBs may take without necessarily establishing an ongoing business relationship for customers:[16]

- Establishing a profile for consumer-enabled transactions;
- Enacting a consumer loyalty program;
- Utilizing features that "recall" information to expedite the processing of transactions; and
- Establishing profiles intended for limited or one-time use.

5. Establishing Due Diligence and Enhanced Due Diligence Standards

MSBs should establish scenarios that will trigger consumer due diligence and enhanced consumer due diligence. These triggering events should be risk-based, incremental, and tailored to the individual MSB. Triggering scenarios may vary based on the types of

[16] For in-person transactions, this includes a review of government-issued identification or other acceptable document and for non-in-person transactions, it may include review of government-issued identification or public records.

[17] The ability to regularly identify consumers through an identifier or account may enable more accurate monitoring and better controls to reduce risk.

transactions or accounts offered.

Examples of potential due diligence include:

- Request that consumers provide or self-certify additional information upon a triggering event (e.g., when transaction over a certain amount);
- Additional document collection for transactions involving higher risk jurisdictions;
- Collection of the purpose for single transactions exceeding specified values; and
- Recordation of additional identifying information after series of transactions.

Examples of potential enhanced due diligence may include:

- Documentation of the source of funds and purpose of the transaction with supporting documentation, if appropriate;
- Utilization of third-party verification services to identify consumers;
- Comparison of transaction patterns to those of other similar consumers; and
- Consumer interviews to gather additional information.

6. Implementing Controls Based on Consumer Activity or Profile

MSBs are required to conduct transaction and consumer monitoring. This monitoring may be implemented in various ways based on the MSB's business model and may include:

- Requiring additional information for transactions to certain jurisdictions;
- Conducting verification for consumers identified to be Politically Exposed Persons ("PEPs"),[17] and
- Limiting transactions or account types based on consumer profiles, such as:
    - Consumers exceeding aggregated transaction values;
    - Consumers located in specific jurisdictions;
    - Consumers conducting rapid receive and send transactions without clear justification; and
    - Consumers conducting transactions that match defined typologies.

Chapter Resources:

- FinCEN's Fund Recordkeeping and Travel Rules:
    - 31 CFR § 1010.410(e)-(f) (https://www.ecfr.gov/cgi-bin/text-idx?SID=dd6ac369c3926f973e618edc945b7984&mc=true&node=pt31.3.1010&rgn=div5#se31.3.1010_1410).
    - FinCEN Advisory Issue 7: "Funds 'Travel' Regulations: Questions & Answers" (January, 1997) (https://www.fincen.gov/sites/default/files/advisory/advissu7.pdf).
- Definition of a Politically Exposed Person:
    - Recommendation 12 of the Financial Action Task Force (June, 2013) (http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-PEP-Rec12-22.pdf).

[18] The FATF's Recommendation 12 defines PEPs as individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, and important political party officials. This definition includes family members who are related to a PEP either directly (consanguinity) or through marriage or similar (civil) forms of partnership, as well as "close associates" who are individuals closely connected to a PEP, either socially or professionally.

Chapter IV
Know Your Agent and Counterparties

1. Overview

As part of an overall AML program an MSB should establish risk-based policies, procedures, and practices to identify agents and counterparties with which it conducts business. These agents and counterparties include, but are not limited to: direct agents, network agents, sub-agents, intermediaries, processors, and referrals. These policies, procedures, and practices should be implemented in accordance with applicable laws and regulations as well as industry guidance, including the *Financial Action Task Force Guidance on a Risk-Based Approach for Money Service Businesses, 2009* and *FinCEN Interpretive Guidance 2004-01- Anti-Money Laundering Program Requirements for Money Services Businesses with Respect to Foreign Agents or Foreign Counterparties.*

2. Definitions

Agent – Any person, excluding officers, directors, or employees of a principal MSB, who acts on behalf of a principal MSB to facilitate the origination or payment of any money services business activity. Example: an electronics retailer or a supermarket store chain selling money orders on behalf of a principal MSB.

Counterparty – A person or entity who has a direct relationship with an MSB to provide products or services to the MSB. Example: a depository institution that provides account and financial services to an MSB.

Direct Agent – A type of agent who has a direct contractual relationship with a principal MSB. Example: a large grocery retailer that directly contracts with an MSB to provide MSB services to the public on behalf of the MSB.

Intermediary – A person who has a direct relationship with a principal MSB to facilitate a money services business transaction and does not directly offer MSB services to the public on behalf of the agent.

Network/Master Agent – An agent that has a direct contractual relationship with a principal MSB and is able to enter into another contractual relationship with a subordinate third-party to allow access to the principal MSB's services. Example: a parent corporation that contracts with multiple

subordinate store chains that, in turn, offer MSB services at their locations (i.e., sub-agents). The MSB services are those that the parent corporation contracted from the principal MSB.

Principal MSB – Any person who directly, or through agents, facilitates the origination, transfer, or disbursement of any money services business activity.

Processor – Any person who facilitates the purchase of, or payment of a bill for, a good or service through a clearance and settlement system by agreement with the creditor or seller. Example: a company that accepts and transmits funds, by contractual agreement, from the public to merchants exclusively for payment of goods and services.

Referral – Any person, not acting in an agent capacity, but in a contractual relationship that refers business to an agent or principal MSB.

Sub-Agent – An agent that has a contractual relationship with a network agent. Example: a supermarket store chain offering MSB services its parent corporation contracted from a principal MSB.

3. Agent and Counterparty Oversight Programs

A. Standards for Agent and Counterparty Due Diligence

MSBs should establish standards for conducting due diligence on their agents and counterparties in accordance with their risk assessments. This due diligence should be conducted using a risk-based approach and should take into consideration the requirements outlined in FinCEN's *Bank Secrecy Act/Anti-Money Laundering Examination Manual for Money Services Businesses.*[18] MSBs should collect and validate the following information on counterparties:

- Name of institution;
- Address of institution;
- Confirmation of license or registration, if required by law;
- Ownership structure identified to the level of 10% owners;
- Names of owners (government-owned or publicly traded companies exempted); and
- Name of Compliance Officer or Compliance point of contact.

In addition to this information, MSBs may also need to gather the following:

- Attestation of an Anti-Money Laundering Program;
- Jurisdictions in which the counterparty operates; and
- Products and services the counterparty provides.

This information collection may be addressed in a variety of ways based on the type and size of the MSB. In addition to conducting due diligence, this information may be useful in performing sanction screening of agents and counterparties. For a small check casher, the relationship may be documented in a physical file indicating the ownership structure that is reviewed on regular basis. For many smaller MSBs, these counterparties and agents may share similar ownership or close familial relationships. For a mid-sized

[19] *See* FinCEN's Bank Secrecy Act/Anti-Money Laundering Examination Manual for Money Services Businesses (2008).

provider of prepaid access, this may include documenting its counterparties, including collecting due diligence information. The Wolfsberg Due Diligence Questionnaire,[19] may assist in ascertaining that the counterparties have AML and sanctions screening policies. For larger money transmitters, information collection processes may include developing a consolidated list of agents and documenting the jurisdictions in which those agents are located and operate.

B. Agent and Counterparty Oversight and Visitation Programs

i. Standards for a Risk-Based Approach of Agent and Counterparty Oversight

In addition to conducting appropriate due diligence for onboarding new agents and counterparties, MSBs should conduct ongoing oversight for agents and counterparties as appropriate based on their risk assessments. This oversight will be different depending on the relationship between the MSB and the counterparty. MSBs should conform to the standards in FinCEN's *Bank Secrecy Act/Anti-Money Laundering Examination Manual for Money Services Businesses*[20] and guidance on compliance obligations for MSB principals[21] and should have policies and procedures for the following:[22]

- Monitoring transactional activity of the agent or counterparty;
- Risk rate agent or counterparties to identify those that may pose higher risk;
- Monitoring and review of adverse media related to the agent entity or its owners, or counterparties;
- Identifying all transactions completed or attempted by agents or counterparties for monitoring purposes;
- Establishing procedures and systems to detect agents or counterparties that may pose elevated risk for financial crime or fraudulent activity;
- Identifying and differentiating activity by individual consumers across various locations, products, and subsidiaries;
- Implementing additional controls for agents or counterparties that demonstrate higher risk activity or are in higher risk corridors;
- Regularly reviewing the due diligence on the agents or counterparties;
- Appropriate training of agents; and
- Confirming that agents or counterparties are properly registered to conduct business.

For smaller money transmitters, this oversight may include manual review of transactions during a defined time period and evaluating the transactions for unusual behavior or transactions. For mid-sized issuers or sellers of money orders, oversight may include developing agent exception reports to evaluate potentially unusual activity due to agent complicity or consumer activity. For larger dealers in foreign exchange, this oversight may involve implementing automated systems to identify agent locations that service consumers that conduct regular transactions and the types of transactions that may be inconsistent with expected activity.

---

[20] *See The Wolfsberg Group Anti-Money Laundering Questionnaire* (June, 2018), *The Wolfsberg Group Anti-Money Laundering Questionnaire* (June, 2018), *and The Wolfsberg Correspondent Banking Due Diligence Questionnaire* (June, 2018).
[21] See supra note 9.
[22] FIN-2016-G001 "Guidance on Existing AML Program Rule Compliance Obligations for MSB Principals with Respect to Agent Monitoring" (March, 2016).
[23] FinCEN's 2017 enforcement action against Western Union Financial Services, Inc. illustrates the need to establish appropriate controls to monitor and guard against illicit activity that may be occurring at agent locations.

ii. Standards for Agent Visitation and Evaluation

In addition to oversight of agents and counterparties, MSBs have a distinct obligation to conduct oversight of agents, including both network agents and sub-agents. At a minimum, principal MSBs should:

- Monitor the transactional activity of individual agents compared to its entire agent population;
- Evaluate agent activity based on consumer fraud complaints;
- Determine higher risk corridors and implement appropriate controls to address the potential risk;
- Conduct additional due diligence on agents that exceed established parameters;
- Review agents periodically to ensure compliance with policy and procedures;
- Understand activity on individual consumers to monitor for agent complicity in illicit transactions; and
- Establish a process to conduct periodic, risk-based onsite agent visits.

The following examples are included for illustrative purposes only: For smaller sellers of prepaid access, agent evaluation and visitation may include regularly scheduled agent site visits as part of ongoing business activities. For mid-sized money transmitters, this may include developing controls to ensure consistent data entry to enhance agent activity reviews. For larger check cashers, this may involve additional due diligence on agent activity not reflective of expected levels for the business type.

iii. Agent Training

MSBs operating under the principal-agent model should develop policies and procedures for their agents to receive appropriate, periodic training. MSBs should ensure the training of its agents covers pertinent federal and state laws and regulations, relevant money laundering and terrorism financing risks and typologies, AML/CFT obligations, and the AML/CFT expectation of agents based on their role.

C. Agent Visitation, Re-authorization, and Terminations

A principal MSB is responsible for the on-going management of its relationship with agents. In general, principal MSBs should visit and review the relationship with its agents based on the risk that they pose to the principal MSB for potential illicit activity. Therefore, each Principal MSB should establish policies and procedures and a schedule for agent visitation/ re-authorization and reviewing its agent relationship based on the risks posed by its agents. Agent visitations and re-authorization should be risk based and may permit offsite or automated policy approvals for agents that are acting within expected parameters. Following a risk-based approach, higher risk agents may merit more frequent visitation or evaluation. FinCEN's *Bank Secrecy Act/Anti-Money Laundering Examination Manual for Money Services Businesses* indicates that periodic visits or reviews of agents' locations may be an indicator of lower overall risk.[23]

[24] See supra note 9.

i. Agent Visitation/Evaluation Schedule

A principal MSB must establish an agent visitation/evaluation program designed to address risk at its agents and ensure ongoing compliance with its policy and procedures on a risk basis. A principal MSB should implement policies or procedures that establish the timeframes and/or parameters for visitations, evaluations, and re-authorizations. A principal MSB can establish criteria and guidelines for agent locations that permit systemic or policy driven re-authorizations that evaluate its agents no less frequently than once every five years. This evaluation process should result in more frequent site visits to the highest risk agents, usually no less often than once per year.

MSBs should establish a process to differentiate risk levels among agents based on factors such as:

- Number of transactions that resulted in Suspicious Activity Reports ("SARs");
- Other unusual transactions;
- Referrals of potentially suspicious agent activity to internal Financial Intelligence Units ("FIUs") or other equivalent teams;
- Volume of activity;
- Geographic risk indicators;
- Agent history;
- Program actions; and
- Other relevant factors.

ii. Agent Visitation/Re-authorization Standards

As applicable, MSBs should establish standard practices for agent visitation/re-authorization in the event that an agent does not qualify for policy-driven or systematic re-authorization. These standards should include the following:

- Review of the due diligence information gathered at agent onboarding;
- Review of the transactional activity conducted by the agent, even if reviewed on a risk basis through other monitoring controls;
- Evaluation and monitoring of the agent's consumers; and
- Confirmation of an ongoing compliance program and adherence to theprincipal MSB's policy and procedures.

iii. Methodology for the Prioritization of Agent Visitations

MSBs should define their methodology to prioritize agent visitations based on a variety of risk-based factors. These factors include, but are not limited to:

- Overall transaction volume activity;
- Geographic risk indicators;
- Number of transactions that resulted in SARs;
- Other unusual transactions;
- Referrals to the FIU/Compliance Staff;
- Number of transactions that resulted in customer fraud; and
- Agent compliance history.

After MSBs establish this methodology for agent visitation, the MSBs should prioritize the frequency and type of visitations based on the risks presented by the various locations. The visitations may be conducted either onsite or performed remotely by the MSB or contracted third party, but the interaction must be well documented to provide the MSB with a sufficient understanding of the practices and activity conducted at the agent location and to serve as evidence to regulators and independent testing parties.

iv. Agent Terminations

MSBs should define procedures and standards for terminating agent relationships. These procedures should prescribe standards and timelines for terminating agent relationships, must clearly indicate the reason for termination and must be commensurate with the risks agents pose to the principal MSB.

Chapter Resources:

- Guidance regarding establishing a risk-based approach:
  - FATF Guidance on the Risk-Based Approach for Money Services Businesses (June, 2009) (http://www.fatf-gafi.org/documents/documents/fatfguidanceontherisk-basedapproachformoneyservicesbusinesses.html).
  - FinCEN Interpretive Guidance 2004-01 "Anti-Money Laundering Program Requirements for Money Services Businesses with Respect to Foreign Agents or Foreign Counterparties." (Dec., 2014) (https://www.fincen.gov/sites/default/federalregister_notice/31cfr12142004.pdf).
- Conducting due diligence on MSB agents and counterparties:
  - FinCEN's Bank Secrecy Act/Anti-Money Laundering Examination Manual for Money Services Businesses (2008) (https://www.fincen.gov/sites/default/files/shared/MSB_Exam_Manual.pdf).
  - 31 CFR § 1010.230 "Beneficial ownership requirements for legal entity customers" (https://www.ecfr.gov/cgi-bin/text-idx?SID=54d4cd9f7a0e00ebe61750bfd0d9e00a&mc=true&node=se31.3.1010_1230&rgn=div8).
  - The Wolfsberg Group Anti-Money Laundering Questionnaire (June, 2018).
  - The Wolfsberg Group Financial Crime Compliance Questionnaire (June, 2018) (https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/Wolfsberg%27s_FCCQ_220218_v1.0.pdf).
  - The Wolfsberg Correspondent Banking Due Diligence Questionnaire (June, 2018) (https://www.wolfsberg-principles.com/wolfsbergcb).
- Monitoring Agents:
  - FinCEN's Guidance FIN-2016-G001 "Guidance on Existing AML Program Rule Compliance Obligations for MSB Principals with Respect to Agent Monitoring" (March, 2016) (https://www.fincen.gov/resources/statutes-regulations/guidance/guidance-existing-aml-program-rule-compliance-obligations).

Chapter V
Reporting and Monitoring

1. Overview

An adequate BSA/AML program must provide for a system of internal controls reasonably designed to prevent, detect, and report potential illicit activity. Regulatory reporting is a visible demonstration of an effective program. In this regard, in addition to relying on independent reviews and internal controls, MSBs can use similar industry peers' AML monitoring and reporting volumes as possible indicators of their AML program's maturity.[24]

In the United States, a reporting program includes two report categories: objective reporting and subjective reporting

2. Definitions

Objective Report – A regulatory report documenting activity that reaches a specific threshold or involves specified jurisdictions. This activity may involve a single transaction or an aggregation of multiple transactions.

[25] MSBs may use FinCEN's Suspicious Activity Report Statistics (www.fincen.gov/reports/sar-stats) as a resource to obtain information on suspicious activity reporting statistics.

Subjective Report – A regulatory report on activity that, in addition to meeting any established minimum threshold, requires an analyst's review and a decision whether to report activity as unusual or possibly suspicious.

3. Report Categories

A. Objective Reports

MSBs have objective reporting requirements when certain thresholds are met or when defined activities occur. As applicable, FinCEN regulations require US MSBs to file four objective report types:

- FinCEN Currency Transaction Reports ("CTRs");
- FinCEN Registrations of Money Services Business ("RMSBs");
- Foreign Bank Account Reports ("FBARs"); and
- Reports of International Transportation of Currency or Monetary Instruments ("CMIRs").

i. Standards for Filing Currency Transaction Reports ("CTRs")

MSBs must file CTRs within 15 calendar days of transactions in currency conducted by or on behalf of a person that exceed $10,000 in one day.[25] CTR filing requirements requires verifying and recording identification. In addition to developing policies and procedures to address the preparation, filing and retention of CTRs MSBs should:

- Ensure systems aggregate activity to identify multiple connected reportable transactions across all product types, locations, and business lines;[26]
- Consider both cash in and cash out;
- Include any fees associated with the transaction totals;
- Establish policies and procedures to comply with identification requirements;[27]
- Implement Quality Assurance processes to verify report accuracy andtimeliness before filing;
- Retain and review records, system-generated reports, and money transmission logs of the transaction or transactions conducted by a customer at single or multiple locations that – including fees – are greater than $10,000 in currency;
- Ensure analysts can refer potential suspicious activity (e.g., structuring) identified during CTR review;
- Submit rules and systems to periodic independent testing;
- Train staff responsible for E-Filing to respond to and potentially escalate submission error notices;
- Review recent enforcement actions and apply lessons learned to reporting processes; and
- Implement a process to document and retain decisions not to file.

[26] *See* 31 CFR §§ 1010.306 and 1010.311.
[27] *See* 31 CFR § 1010.313.
[28] *See* 31 CFR § 1010.312.

ii. Standards for Submitting Registrations of Money Services Business ("RMSBs")

Registration with FinCEN as an MSB is required for businesses engaged in activities described in 31 CFR § 1010.100(ff). Companies should consider, as appropriate:

- Seeking and documenting a legal opinion determining the requirement to register;
- Although renewal registration is only required every other year, consider renewing on an annual basis to avoid missed submissions;
- Retain a copy of all the information contained within the actual registration instead of just retaining the confirmation of registration; and
- Keep in one file all required supporting documents (the entire registration form, the annual estimate of volume, ownership of the business, and the complete agent list) rather than relying on these pieces of information to be on file "somewhere" in the company.

iii. Standards for Filing Foreign Bank Account Reports ("FBARs")

MSBs with financial interest or signature authority over an account in a foreign country that exceeds $10,000 at any time during the calendar year are required to file Foreign Bank Account Reports (FBARs) annually.[28, 29] Companies should:

- Train individuals in corporate Treasury departments who will be responsible for tracking and completing the FBAR;
- Ensure that owners with signature authority complete the FBAR annually;
- Understand that there is no penalty for overreporting and no penalty for individuals who report when they did not need to, so it is best to interpret terms such as "Persons," "Accounts," and "Authorities" as broadly as possible; and
- Assemble a team that includes representatives from Treasury, HumanResources, Legal, and Tax to administer the FBAR process.

iv. Standards for Reports of International Transportation of Currency or Monetary Instruments ("CMIRs")

In general, the BSA requires that a CMIR be filed when currency, or other monetary instruments, in an aggregate amount exceeding $10,000 is physically transported, mailed, or shipped from the United States to any place outside the United States or into the United States.[30] While limitations apply,[31] the BSA has not exempted MSBs from CMIR filing requirements. Accordingly, an MSB should:

- Review its functions, products, and services to determine whether any of its operations require the filing of a CMIR and
- Establish policies and procedures to, and train individuals in corporate Treasury departments who will be responsible for, tracking and completing in a timely fashion the CMIR.

---

[29] *See* 31 CFR § 1010.350.
[30] On December 16, 2016, FinCEN released information on a new annual due date for FBAR filings. The due date is now April 15 to coincide with the Federal income tax filing deadline.
[31] *See* 31 CFR § 1010.340 and the CMIR General Instructions.
[32] 31 CFR § 1010.340(d) indicates that a transfer of funds through normal banking procedures, which does not involve the physical transportation of currency or monetary instruments, is not required to be reported.

B. Subjective Reports

i. Standards for Filing Suspicious Activity Reports ("SARs")

To assist government and law enforcement agencies in combating terrorist financing, money laundering, and other financial crimes, MSBs must electronically report to FinCEN any suspicious transaction relevant to a possible violation of law or regulation within 30 calendar days of knowing, suspecting, or having reason to suspect that an activity/transaction is suspicious.[32, 33] 31 CFR §§ 1010.314 and 1022.320 outline when activity and transactions would be reported as suspicious.

Certain factors, such as the dollar amount of activity and the type of service(s) provided by the MSB, dictate the specific SAR filing requirements. MSBs should adhere to FinCEN's standards outlined in the *Bank Secrecy Act/Anti-Money Laundering Examination Manual for Money Services Businesses* and should implement policies and procedures to:

- Allow and encourage referrals of unusual activity from all teams within the company as well as from agents;
- Create clear, minimum standard language to be included in all SAR narratives, including FinCEN's key terms outlined in SAR Advisories;
- Manage/limit access by identifying individuals with a need to access SARs;
- Include the date of detection in the narrative;
- Create a well-defined SAR review process or team;
- Implement a Quality Assurance processes to verify report accuracy and timeliness before filing;
- Perform periodic testing of completed filings to ensure reports are completed accurately and timely;
- Train staff responsible for E-Filing to respond to and potentially escalate submission error notices;
- Communicate potential complicit agent activity to teams responsible for corrective action, escalations, and agent terminations;
- Report SARs and suspicious activity to senior management;
- Store SARs and SAR-related information in restricted access/password-protected files;
- Perform periodic user access reviews;
- Review recent enforcement actions and apply lessons learned to reporting processes; and
- Implement a process to document and retain decisions not to file.

C. Sanctions

MSBs also have the obligation to comply with laws and regulations administered by the US Department of the Treasury's Office of Foreign Assets Control ("OFAC"). OFAC administers a series of laws that impose economic sanctions against individuals, companies, and countries to further US foreign policy and national security objectives.[34] This means that MSBs (like any other US person and financial institution) are not permitted by law (administered through OFAC) to conduct business with a sanctioned

[33] *See* 31 CFR § 1022.320.
[34] Please see the FinCEN's FAQs Regarding the FinCEN SAR for information on how to electronically file SARs.
[35] *See* "OFAC Regulations for the Financial Community."

party. It is important to note that compliance with OFAC's rules and regulations is governed under strict liability. In addition, each MSB is responsible for the transactions processed through its systems and it cannot reallocate its liability to a third party. Thus, an MSB should have effective policies and procedures and sanctions screening program to seek to ensure compliance with OFAC's rules and regulations.

As part of their sanctions compliance obligations, upon identifying transactions that may involve a sanctioned party, MSBs must, as required, block or reject the transaction, and subsequently report such transactions in accordance with applicable sanctions rules and regulations.[35] Certain rules and regulations may require that an MSB segregate funds into a separate, interest-bearing account ("blocked account"), and may require that the MSB file immediate and annual reports providing an accounting of the blocked property held in its blocked account.[36] The transfer of blocked funds held at one depository institution to another depository institution will require OFAC authorization in the form of a specific OFAC license.[37]

MSBs may seek government advice before making a final determination on whether to block or reject a transaction, such as in cases where the MSB is unable to determine whether there is a true match to a sanctions list. MSBs, however, should not conduct/complete a transaction if they are unsure the involved parties are not sanctioned by OFAC. MSBs must implement procedures and controls for reporting blocked and rejected transactions in accordance with the applicable government sanctions programs, and for other required reporting such as an annual reporting of blocked funds.[38]

i. Standards for Filing Reject and Block Reports with OFAC

- Develop clear, minimum standard language for reject and block reports that would be filed with OFAC within 10 business days;[39]
- Obtain and retain a copy of internal screening records in accordance with recordkeeping requirements;[40]
- Keep all required supporting documentation in a centralized location and in accordance with recordkeeping requirements;[41]
- Maintain an ongoing tracker for all filed reports to document transaction, transactor, and recipient information, as well as, any internal screening data that can assist with the MSB's risk assessment;
- Communicate potential complicit insider/internal/agent activity to teams responsible for corrective action, escalations, and terminations;
- Document and retain any remedial actions taken, such interdicting parties involved with the rejected and/or blocked payment, corrective action taken, procedural updates and/or system fixes; and
- Perform periodic testing of completed report filings to ensure reports are completed accurately and timely.

[36] *See* 31 CFR § Part 501 – Reporting, Procedures and Penalties Regulations.
[37] *See* 31 CFR § Part 501.603 – Reports on blocked property.
[38] *See* 31 CFR § Part 501.801 – Licensing.
[39] *See* 31 CFR §§ Part 501.603 – Reports on blocked property and 501.604 – Reports by US financial institutions on rejected funds transfers.
[40] *See* 31 CFR §§ Part 501.603 – Reports on blocked property and 501.604 – Reports by US financial institutions on rejected funds transfers.
[41] *See* 31 CFR § Part 501.601 – Records and recordkeeping requirements.
[42] Id.

ii. Standards for Blocking Property

- Under certain sanctions programs, MSBs are required to block (i.e., freeze) the property and assets of specific governments, entities, or individuals. The definition of property and assets is often broad and is specifically defined within each sanctions program;
- Similarly, under certain sanctions programs, the blocked property would need to be placed in an interest-bearing account at a depository financial institution and cannot be moved, cancelled, or amended without authorization from OFAC;[42] and
- Complete monthly reconciliation of the interest-bearing account(s) to ensure proper accounting of blocked property and accurate recordkeeping.

iii. Standards for Filing Annual Report of Blocked Property to OFAC

- 31 CFR § 501.603 requires persons holding property blocked per OFAC sanctions and regulations to provide OFAC, by September 30 of every year, with a comprehensive list of all blocked property held as of June 30 of that year (known as an Annual Report of Blocked Property ("ARBP"));
- Property that has been unblocked by a general or specific OFAC license, but that has not been returned to its owner, is should not be considered blocked property or reported to OFAC in the ARBP;
- The annual reports must be filed by the MSB (not by the depository institution where the MSB's interest bearing account is held) using Form TD F 90-22.50 via email to OFACReporting@treasury.gov, and the MSB should retain record of any filing/submission confirmation provided by OFAC;
- Perform periodic testing of completed filings to ensure reports are completed accurately and timely; and
- Keep all required supporting documentation in a centralized location and in accordance with recordkeeping requirements.[43]

4. Monitoring

MSBs have an obligation to design a risk-based program to monitor for suspicious activity as defined in 31 CFR § 1022.320. Similar to other financial institutions, MSBs must develop a risk-based program based on the size and complexity of their business. These systems may be automatic or manual dependent on the risks the MSB is attempting to mitigate.

A. Control Categories

Generally, there are nine types of transaction monitoring controls for MSBs to consider when mitigating AML/CFT and fraud risks.

i. Data Collection Controls for Originators and Receivers

Data collection controls are designed to ensure that MSBs collect appropriate information to process the transaction and that this information is in an acceptable format. In many cases, MSBs will collect this information as part of the normal course of business. Appropriate data collection controls facilitate all other controls.

[43] Please refer to each specific sanctions programs for requirements about placing blocked property in interest-bearing accounts. For example, refer to 31 CFR § 560.213 for Iranian transactions and sanctions regulations.
[44] 31 CFR § 501.603 requires records to be kept no less than five years after the date of the transaction.

As applicable, based on the MSB's risk assessment, the following information should generally be collected for most MSB transactions:

- Complete name of the transactor;
- Location (e.g., physical address) of the transactor;
- Amount of the transaction;
- If applicable, name of receiver; and
- An identification reference or number for the transaction.

ii. Screening Controls/Sanctions

Screening controls are rules designed to identify and appropriately restrict or prohibit transactions involving parties with whom it is impermissible to conduct business, or parties with whom MSBs have chosen not to conduct business. These parties may include:

1. Parties included in government sanctions lists (e.g., OFAC); or
2. Parties with which the MSB has made a risk decision (e.g., AML, Fraud, Credit, PEP) to prevent these parties from completing transactions.

Screening controls may be automated or manual, based on the type of business in which the MSB engages. Where possible, sanctions screening should be conducted prior to a transaction being processed/accepted.[44] Additionally, potential sanctions matches should be resolved prior to transactions being cancelled and funds returned to the transactor.

Mirroring OFAC's sanctions list search tool, MSBs should consider using "fuzzy logic" as part of their sanction screening tools.[45] Fuzzy logic uses character and string matching as well as phonetic matching. This logic traditionally deploys comprehensive parameters to take into account linguistic differences.

iii. Enhanced Data Integrity Controls

Enhanced Data Integrity Controls are designed to ensure the data collected at the time of the transaction is in the correct format and reasonably accurate. These controls can be applied in a manual or automatic fashion to various information and customized to jurisdictions and other variables as needed.

iv. Originator Limit Controls

Because the portfolio of products offered by MSBs differs from traditional banking products, and MSBs themselves offer a wide range of products, the controls or restrictions put in place by MSBs may be different from those implemented by other financial institutions to manage the distinct risks. For these reasons, MSBs may opt to place jurisdictional and transaction limits on their products. Those limits may be triggered at the point of sale and be supported by system restrictions that prevent exceeding established limits. Limits should consider single transactions as well as transactions in aggregate.

[45] The 2015 enforcement action taken by OFAC against PayPal, Inc. exemplifies the need to conduct sanctions screening prior to a transaction being processed or accepted by an MSB.
[46] See OFAC's Sanctions List Search Tool (https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/fuzzy_logic.aspx).

Originator Limit Controls may stop transactions or provide notification to the consumers. These may include:

- Single transaction rules based on the data elements entered during the transaction and/or the dollar amount of the transaction that result in the transaction being stopped at the point of sale.
- Aggregate transaction rules based on the data elements entered during the transaction and/or the dollar amount of the transactions that result in the transaction being stopped at the point of sale.

Data elements may include specific jurisdictions, thresholds, timeframes, product types, consumer biographical information or location.

v. Receiver Limit Controls

Receiver Limit Controls are single or aggregate transaction rules that may stop transactions or provide notification to the consumer.

vi. Behavioral Suspension and Queueing Controls

Behavioral Suspension and Queuing Controls are single or aggregate transaction rules that suspend a transaction and place it in a queue for further investigation and/or a consumer interview.

vii. Transaction Surveillance Controls

Transaction Surveillance Controls are single or aggregate transaction rules that include completed transactions and may include attempted transactions. These rules may require reporting to local regulators based on jurisdictional regulations or risk-based analysis.

viii. Exception Reports

Exception Reports identify unusual transaction patterns based on variable risk factors within jurisdictions or groups of consumers, such as previous investigative results, law enforcement information, and geo-political events.

ix. Risk Models

Risk Models are models that deploy a risk-based approach in assessing indicators of AML/CFT/Fraud risk. Models may utilize a variety of statistical frameworks, including predictive and prescriptive scoring methods, whereby risk factors are evaluated to provide a probability of a subject's risk or a stack risk rank of a population. Such models allow for several risk factors to be evaluated simultaneously and provide for robust outlier detection to identify, evaluate, and decision risk within a specific population.

Chapter Resources:

- Currency Transaction Reports (CTRs) requirements:
  - 31 CFR § 1010.311 (https://www.ecfr.gov/cgi-bin/R?gp=&SID=54d4cd9f7a0e00ebe61750bfd0d9e00a&mc=true&n=pt31.3.1010&r=PART&ty=HTML#se31.3.1010_1311).
- MSB registration requirements:
  - 31 CFR § 1010.100 (ff) and 1022.380 (https://www.ecfr.gov/cgi-bin/=0c48a68807544cc3b04f009e37b08a00&mc=true&node=se31.3.1010_1100&rgn=div8).

- Reports of foreign financial accounts (FBAR) requirements:
  - 31 CFR § 1010.350 (https://www.ecfr.gov/cgi-bin/R?gp=&SID=0c48a68807544cc3b04f009e37b08a00&mc=true&n=pt31.3.1010&r=PART&ty=HTML#se31.3.1010_1350).
  - Annual deadline to file FBARs (https://www.fincen.gov/sites/default/files/2016-12/New%20FBAR%20Due%20Date%20Announcement%20%28FINAL%2012-16-16%29.pdf).
- Suspicious Activity Reports (SARs) requirements:
  - 31 CFR § 1010.314 (https://www.ecfr.gov/cgi-bin/R?gp=&SID=0c48a68807544cc3b04f009e37b08a00&mc=true&n=pt31.3.1010&r=PART&ty=HTML#se31.3.1010_1314).
  - 31 CFR § 1022.320 (https://www.ecfr.gov/cgi-bin/text-idx?SID=0c48a68807544cc3b04f009e37b08a00&mc=true&node=pt31.3.1022&rgn=div5#se31.3.1022_1320).
  - FinCEN's Bank Secrecy Act/Anti-Money Laundering Examination Manual for Money Services Businesses (2008) (https://www.fincen.gov/sites/default/files/shared/MSB_Exam_Manual.pdf).
  - Frequently Asked Questions Regarding the FinCEN SAR (https://www.fincen.gov/frequently-asked-questions-regarding-fincen-suspicious-activity-report-sar).
- Suspicious Activity Reports (SARs) Statistics:
  - FinCEN's SAR Stats (www.fincen.gov/reports/sar-stats).
- Sanctions:
  - OFAC Regulations for the Financial Community (https://www.treasury.gov/resource-center/sanctions/Documents/facbk.pdf).
  - OFAC's Sanctions List Search Tool (https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/fuzzy_logic.aspx).
  - 31 CFR § Part 501 – Reporting, Procedures and Penalties Regulations (https://www.ecfr.gov/cgi-bin/text-idx?SID=0c48a68807544cc3b04f009e37b08a00&mc=true&node=pt31.3.501&rgn=div5).
  - 31 CFR § Part 501.601 – Records and recordkeeping requirements (https://www.ecfr.gov/cgi-bin/text-idx?SID=0c48a68807544cc3b04f009e37b08a00&mc=true&node=pt31.3.501&rgn=div5#se31.3.501_1601).
  - 31 CFR § Part 501.603 – Reports on blocked property (https://www.ecfr.gov/cgi-bin/text-idx?SID=0c48a68807544cc3b04f009e37b08a00&mc=true&node=pt31.3.501&rgn=div5#se31.3.501_1603).
  - 31 CFR § 501.604 – Reports by US financial institutions on rejected funds transfers (https://www.ecfr.gov/cgi-bin/text-idx?SID=0c48a68807544cc3b04f009e37b08a00&mc=true&node=pt31.3.501&rgn=div5#se31.3.501_1604).
  - 31 CFR § Part 501.801 – Licensing (https://www.ecfr.gov/cgi-bin/text-idx?SID=0c48a68807544cc3b04f009e37b08a00&mc=true&node=pt31.3.501&rgn=div5#se31.3.501_1801).

Chapter VI
Information Sharing

1. Overview

Section 314 of the USA PATRIOT Act of 2001 establishes mechanisms for cooperative sharing of information between financial institutions, law enforcement agencies, and regulators. The regulations provide safe harbor from liability to institutions participating in the information sharing program under Section 314(b).

The ability to share information assists agencies to deter, detect, and investigate activities potentially related to money laundering and terrorist financing.

In addition to using information sharing tools to communicate with external parties (law enforcement, regulatory agencies, and other financial institutions), MSBs should implement ways for internal departments to share information.

2. Section 314 of the USA PATRIOT Act

A. Section 314(a) of the USA PATRIOT Act and 31 CFR § 1010.520

FinCEN has asked certain MSBs to participate in this type of information sharing, and all MSBs should at least be aware of the process as regulators may inquire about it during examinations. Larger MSBs receive, every other week, email notifications, as well as occasional ad hoc notifications from FinCEN's Secure Information Sharing System ("SISS"). If an MSB is asked to participate in this information sharing, it should:

- Register to participate using FinCEN's SISS website;[46]
- Determine the appropriate point(s) of contact at the company to receive and respond to notifications, and ensure there is more than one person aware of and trained on the process and requirements;
- Develop written procedures that address:
  - Search parameters such as types of records and timeframes;
  - Positive match reporting deadlines;
  - 314(a) search impacts on account closures, interdictions, and Suspicious Activity Reporting;
  - Confidentially requirements; and

[47] Available at https://www.fincen.gov/314a/Login.

  - Recordkeeping requirements.
- Create a log to serve as evidence to examiners and auditors that searches are performed, and matches reported on time.

Once a request is received, MSBs should ensure they:

- Perform a one-time search of the required records; and
- Report any positive matches to FinCEN within 14 days.

B. Section 314(b) of the USA PATRIOT Act and 31 CFR § 1010.540

Section 314(b) of the USA PATRIOT Act provides financial institutions with the ability to share information with one another, under a safe harbor that offers protections from liability, in order to better identify and report potential money laundering or terrorist activities.[47]

Section 314(b) information sharing is voluntary. However, FinCEN strongly encourages participation, and in November 2016 published a "Section 314(b) Fact Sheet" highlighting the benefits of sharing among financial institutions, which was more recently updated in December 2020.[48]

MSBs should discuss and document the management decision to participate and then implement policies and procedures to ensure:

- The MSB registers initially and annually thereafter on FinCEN's SISS designating a point of contact to participate;[49]
- Both the requesting financial institution and responding financial institution have registered with FinCEN prior to sharing any information and evidence is retained that this is verified with each request received;
- The information exchanged is related only to money laundering or terrorist financing suspicions;
- Processes are developed for deciding when and if to file a SAR relative to requests;
- Facts related to actual SAR filing decisions are not shared with other participating institutions;
- Confidentiality is maintained;
- Overseas information sharing with non-US financial institutions is not permitted;[50] and
- Records are retained for at least 5 years.[51]

[48] See FinCEN's Section 314(b) Fact Sheet (December, 2020).
[49] Id.
[50] MSBs may register at https://www.fincen.gov/314b/Register.
[51] FinCEN's Section 314(b) Fact Sheet specifies that only financial institutions subject to an AML program requirement under FinCEN regulations, and any association of such financial institutions, are eligible to share information under Section 314(b).
[52] FinCEN's regulations establish recordkeeping requirements related to various types of records, including for records that document an MSB's compliance with the BSA. In general, FinCEN's regulations require financial institutions to maintain records for at least 5 years. Accordingly, as a best practice, MSBs may consider retaining information shared under Section 314(b) for a 5-year period.

3. Regulatory Information Sharing

FinCEN has the authority to issue a summons for information to MSBs.[52] If an agency like FinCEN requests data, MSBs should be prepared to respond to these requests and MSBs should have established processes for responding to such requests.

4. Law Enforcement Information Sharing

Law enforcement agencies may also request information from MSBs, such as SAR supporting documentation, under their authorities as part of conducting an investigation. FinCEN has clarified that the BSA provides protection from civil liability for all reports of suspicious transactions made to appropriate authorities, including supporting documentation, regardless of whether such reports are mandatory.[53] Thus, MSBs should have appropriate policies and procedures for complying on a timely manner with requests from appropriate law enforcement to provide information.[54]

Similarly, law enforcement agencies may request MSBs to continue providing services to certain individuals or entities despite exhibiting potential suspicious activity. Ultimately, the decision to provide services should be made by the MSB in accordance with its own standards and guidelines. Although there is no requirement that an MSB maintain a particular relationship, MSBs should be mindful that complying with such a request may further law enforcement efforts to combat money laundering, terrorist financing, and other crimes. If a law enforcement agency requests that a financial institution maintain a particular account, the financial institution should ask for a written request detailing the specifics of such request, such as its expiration.[55]

5. Internal Information Sharing

Within each MSB, there are often multiple departments or teams with access to information that could be useful to the Compliance Department staff and to detecting suspicious activity. MSBs should take steps to ensure that all available information is shared with Compliance. Appropriate Compliance staff should have direct access to as much information as possible, as this information can play an important role in determining risk and identifying potentially illicit activity.

Employees across the company should receive BSA/AML training that provides:

- Understanding of the types of activity each employee could witness that could be considered unusual; and
- Ways to refer potentially suspicious activity to Compliance.

The types of departments to consider for purposes of internal information sharing include:

- Fraud groups;
- Agents;
- Sales teams;
- Customer service representatives;
- Information Technology teams (especially their knowledge of cyber-events);

[53] *See* 31 CFR §§ 1010.911, 1010.912, and 1010.913.
[54] *See* 31 U.S.C. § 5318(g)(3) and FinCEN's guidance FIN-2007-G003: "Suspicious Activity Report SupportingDocumentation" (June, 2007).
[55] *See* FinCEN's "Providing Suspicious Activity Reports to Appropriate Law Enforcement," SAR Activity Review: Trends, Tips & Issues, Issue 9, p.43 (Oct., 2005); FIN-2007-G003: "Suspicious Activity Report Supporting Documentation" (June, 2007); and Appendix F of the BSA/AML Examination Manual for MSBs (2008).
[56] For further information please refer to FinCEN's guidance FIN-2007-G002: "Requests by Law Enforcement for Financial Institutions to Maintain Accounts" (June, 2007).

- Affiliates; and
- Legal departments.

6. Sections 314(a) and (b) SAR Disclosure Limitations

MSBs should have processes in place to determine whether a SAR should be filed in relation to information requests. However, regardless of the source of request for information, the MSB is prohibited from disclosing whether a SAR has been filed relative to any related investigations. Sections 314(a) and (b) of the USA PATRIOT Act do not authorize MSBs to share SARs or to disclose the existence or nonexistence of a SAR.[56] If an MSB learns of an unauthorized SAR disclosure, FinCEN should be notified.

Chapter Resources:

- Section 314(a) of the USA PATRIOT Act:
  - 31 CFR § 1010.520 "Information sharing between government agencies and financial institutions" (https://www.ecfr.gov/cgi-bin/text-idx?SID=b16a3a75156d69185d127b970cbed9fd&mc=true&node=pt31.3.1010&rgn=div5#se31.3.1010_1520).
  - Registering to participate in 314(a) information sharing and FinCEN's SISS (https://www.fincen.gov/314a/Login).
- Section 314(b) of the USA PATRIOT Act:
  - 31 CFR § 1010.540 "Voluntary information sharing among financial institutions" (https://www.ecfr.gov/cgi-bin/text-idx?SID=b16a3a75156d69185d127b970cbed9fd&mc=true&node=pt31.3.1010&rgn=div5#se31.3.1010_1540).
  - Registering to participate in 314(b) information sharing and FinCEN's SISS (https://www.fincen.gov/314b/Register).
  - FinCEN's Section 314(b) Fact Sheet (December, 2020) (https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf).
- Providing information to government agencies:
  - 31 CFR §§ 1010.911, 1010.912 and 1010.913 "Summons" (https://www.ecfr.gov/cgi-bin/text-idx?SID=b16a3a75156d69185d127b970cbed9fd&mc=true&node=pt31.3.1010&rgn=div5#sp31.3.1010.i).
  - FinCEN's guidance FIN-2007-G003: "Suspicious Activity Report Supporting Documentation" (June, 2017) (https://www.fincen.gov/sites/default/files/shared/Supporting_Documentation_Guidance.pdf).
  - FinCEN's "Providing Suspicious Activity Reports to Appropriate Law Enforcement," SAR Activity Review: Trends, Tips & Issues, Issue 9, p.43 (Oct., 2005) (https://www.fincen.gov/sites/default/files/shared/sar_tti_09.pdf).
  - FinCEN's guidance FIN-2007-G002: "Requests by Law Enforcement for Financial Institutions to Maintain Accounts" (June, 2007) (https://www.fincen.gov/sites/default/files/shared/Maintaining_Accounts_Guidance.pdf).
  - Appendix F of the BSA/AML Examination Manual for MSBs (2008) (https://www.fincen.gov/sites/default/files/shared/MSB_Exam_Manual.pdf).

[57] Please refer to sections 3 and 4 of this chapter for information regarding authorized sharing of SARs with appropriate law enforcement and regulatory agencies.

Chapter VII
Licensing Requirements

1. FinCEN Registration

MSBs are required to register with FinCEN and ensure at all times that their registration remains current. Certain events trigger re-registration, and registration must be renewed every two years. Entities that are MSBs solely because they are an agent of another MSB are not required to register.[57]

Foreign-located person doing business in the United States as an MSB must also register with FinCEN and designate a person who resides in the United States to be an agent to accept service of legal process.[58]

MSBs, including foreign-located MSBs, must comply with regulations under the BSA, including the maintenance of an adequate AML program.

2. State Licensing

State licensing requirements vary considerably by state and should be analyzed based on the product types and business structure. Some states may require multiple licenses for a single MSB, and some may not require any, depending on the facts and circumstances of a given company's products and operations.

The types of activities generally requiring state licensure include:

- Check cashing;
- Transmitting/receiving funds for transmission;
- Exchanging currency (including virtual currency);
- Selling or issuing prepaid access or stored value; and
- Selling or issuing of monetary or payment instruments, such as travelers checks or money orders.

If an MSB is engaged in these activities, an evaluation of licensing requirements in each state should be conducted. License types may include currency exchanger, money transmitter, check casher, check seller, or virtual currency/BitLicense. A company may need a license in a state even if it does not meet the federal definition of an MSB. State definitions of the above activities are often different from those in the BSA, because state statutes are generally grounded in consumer protection and safety and soundness, whereas the BSA's focus is on the prevention of money laundering.

[58] *See* 31 CFR § 1022.380.
[59] See 31 CFR § 1022.380(a)(2).

It is important to note that state licensing is generally location-agnostic, meaning that a company need not have a physical presence in a given state to require a license. If a company is providing a regulated product to consumers in a particular state, licensure is often required regardless of where the company is physically located.

MSBs should be aware that banks and other financial institutions they may partner with usually request MSBs' licensing information for their records. Accordingly, MSBs should readily maintain this information.

A. Applying for a State License

Unlike the federal FinCEN registration, an MSB must apply for and receive approval for a state license. This involves completing an application (often through a nationwide licensing system—NMLS), remedying any deficiencies noted by the state, and possibly submitting additional documentation. Prior to submitting a state application form, most MSBs must complete the following and may be required to submit some or all of these documents:

- Documented business plan, strategy, and financial forecast;
- State business license, articles of incorporation, and information on principals and owners;
- Proposed agents or authorized delegates and sample contracts;
- Source of funding, current financial statements and historical financial statements (3 years of audited financials);
- Bank account information;
- Copies or screen prints of receipts, invoices, and other customer-facing documentation;[59]
- AML program;
- Surety bond;
- Sample payment instruments; and
- Due diligence and background and credits checks on officers, directors, and controlling persons.

Some states will grant a provisional license, which requires an MSB to follow more stringent requirements for a specific amount of time when it first receives a license.

B. Maintaining a License

Once an MSB receives a license, it must take proactive steps to maintain its license. Maintaining licenses generally involves:

- Notifying states of any changes in control or other major business changes;
- Complying with any approval conditions imposed by the state;
- Maintaining adequate shareholder equity;
- Maintaining a safe and sound financial condition;

[60] Some states may require pre-approval of receipt templates prior to use.

- Filing and paying annual assessments and license renewals;
- Filing monthly, quarterly, annual reports (including annual audited financial statements);
- Maintaining surety bonds in compliance with each state requirement;
- Being subject to state compliance and safety and soundness examinations and remediating findings; and
- Complying with all state and federal regulatory requirements.

Chapter Resources:

- Requirement for MSBs to register with FinCEN:
  - 31 CFR § 1022.380 "Registration of money services businesses" (https://www.ecfr.gov/cgi-bin/text-idx?SID=b16a3a75156d69185d127b970cbed9fd&mc=true&node=pt31.3.1022&rgn=div5#se31.3.1022_1380).
  - FinCEN's MSB registration webpage (https://www.fincen.gov/money-services-business-msb-registration).

Chapter VIII
Compliance Certifications (Optional)

1. Overview

This chapter offers information to MSBs operating in the state of New York, which requires financial institutions to annually certify their AML programs to ensure their effectiveness. As of this writing, in the United States, New York is the only state requiring such annual certification; however, other states and jurisdictions may implement similar certification requirements in the future.

A compliance certification process involves program testing and ongoing assessment to ensure the BSA/AML program continues to comply with regulatory expectations. Establishing a diagnostic of the AML program is key to positioning an MSB, namely the board of directors or a senior officer, to provide appropriate certification of compliance requirements. As described in Chapter II, MSBs should employ the three-lines-of-defense model to ensure appropriate departments, such as the business lines, are stakeholders and actively engaged in any certification process.

Poorly executed certifications can expose the Board or senior officer to significant risk if certifications are based upon incomplete or inaccurate data, a faulty system, or a faulty assessment of the system. The following steps illustrate an example of a documented approach for MSBs to develop a compliance certification process.

2. Identify and Document Compliance Certification Requirements

The process for building a compliant BSA/AML Program is as important as the execution of the certification. Institutions should develop a detailed action plan, including deadlines and key milestones for evaluating the requirements of the compliance certification. Institutions may find that experienced counsel can provide value by assisting the institution in understanding the regulatory expectations and navigating issues such as the application of competing AML regulations in other jurisdictions. When determining how best to move forward, it is important to consider a framework responsive to the requirements of the compliance certification. MSBs should ensure that adequate documentation is maintained to articulate any assumptions, parameters, and thresholds when determining compliance certification requirements.

3. Determine Scope

Because MSBs range from larger, multinational companies to smaller businesses, they may offer a wide variety of products and services carrying varying degrees of risk. Therefore, MSBs should create an inventory of all products their business models offer and then understand the applicability of such products towards a given compliance certification. The business line or operational management should certify any product list.

4. Validate Data, Systems, and Processes

After having determined the scope of the compliance certification, MSBs should continue to ensure their understanding of their transactions' lifecycle as well as any processes (manual and automated) and systems that make up such lifecycle. MSBs must identify where and how data is initially captured, and how it is extracted, transformed, channeled, and loaded to various systems throughout the entire lifecycle of a transaction. Institutions should additionally be able to identify where the data they use has come from and substantiate its quality. Records and documents should be created and maintained to regularly validate data sources and map processes. In support of compliance certifications, MSBs should review system functionality, settings, and limitations, while evaluating existing change control processes.

5. Test Compliance Systems for Effectiveness

The next step in a compliance certification should involve MSBs clearly identifying the AML controls they use to ensure completeness and accuracy of compliance processes. Whether such controls are systematic or manual, preventive, proactive or reactive, these must be clearly documented, be the responsibility and accountability of specific persons, and be subject to monitoring, whether ongoing or specific. It is from this set of AML controls that effective independent testing can be formulated and conducted in support of the compliance certification. Demonstrability is critical, as the Board or senior officer must be well informed and able to attest to the effectiveness of the AML program (e.g., model workflow from transaction generation to the disposition of alerts).

6. Review Audit, Examination, and Testing Findings for Deficiencies

MSBs should undergo periodic testing of the effectiveness of their AML program and its compliance with legal and regulatory requirements to prevent, detect, and report money laundering, terrorist financing, and other illegal activity. Gaps should be clearly identified, detailed remediation plans put in place and documented, including clear milestones and evidence any remediation plans are implemented and completed.

7. Document Planned Enhancements

MSBs should then evaluate AML program processes and controls relevant to a compliance certification to identify potential gaps/issues. MSBs should compile reports in support for the compliance certification, including remedial efforts planned or in-process to address identified weaknesses or deficiencies. Sufficient remediation should be completed to have programs that are reasonably designed to address identified risk, which should be the basis for a certification that is based on a reasonable and rational judgment. In cases where the extent and speed of remediation is dependent upon the size and significance of the gap, ongoing action plans may be necessary where remediation cannot be completed prior to certification.

8. Certify the Program

Certification is the culmination of these various efforts (above). The Board or senior officer should be able to determine whether the organization has executed a reasonably informed, good faith, rational judgment without the presence of a conflict of interest. To reach this conclusion, the AML program must rely on a robust compliance certification framework. The Board or senior officer must set the standards under which the AML program can be considered as reasonably designed to prevent, detect, and report potential illicit activity. Further, there must be sustainable governance and oversight mechanisms in place to monitor the effectiveness of the AML program, including policies and procedures.

Chapter Resources:

- New York Department of Financial Services' "Transaction Monitoring Certification (504)" (https://www.dfs.ny.gov/industry_guidance/transaction_monitoring).
- New York Department of Financial Services' submission secure portal (https://myportal.dfs.ny.gov/welcome?p_p_state=maximized&p_p_mode=view&saveLastPath=false&_58_struts_action=%2Flogin%2Flogin&p_p_id=58&p_p_lifecycle=0&_58_redirect=%2Fweb%2FRegulations-504).