COMPLY ADVANTAGE®

Securing and Maintaining a Healthy Banking Relationship: A Guide for MSBs

Obtaining banking services as a Money Service Business (MSB) or fintech providing services similar to an MSB can be challenging. Some banking service providers are more reluctant to work with these types of businesses due to the higher inherent risks of money laundering and terrorist financing. Banking service providers may also have strict application requirements and high fees. Only MSBs and fintechs with robust operations and solid, proven KYC and AML compliance programs are usually considered and accepted as clients.

We've created this guide to help you achieve this goal by drawing on the experience of our regulatory and compliance experts, in-house practitioners who have advised MSBs and fintechs. We have also drawn on our experience serving banks and banking service providers with fintech/MSB service programs. Before applying for services, it can be difficult to know whether a given business will meet the criteria to be accepted as a client. We've created this guide to maximize firms' chances of achieving this goal.

We'll set out the categories banking service providers will consider when reviewing applications and our advice on how firms can position themselves for success. The areas we will focus on are:

- Compliance Program Completeness
- Business Activities
- Financial Fitness
- Legal Fitness
- Audit Track Record

Compliance Program Completeness

The first step firms must take is to demonstrate a proven, robust compliance program. This sets the tone for the relationship with banking service providers, building trust with the assessment team. All required components will be verified for accuracy and completeness.

This includes the appointment of an experienced, qualified Head of Compliance. Whether their title is Chief Compliance Officer, Money Laundering Reporting Officer, Bank Secrecy Act (BSA) Officer, or an equivalent, this person must have relevant experience in running a compliance team and program in order to be seen in the most favorable light during the application process.

When documenting its compliance program, every firm should include:

AML policies and procedures detailing a business's obligations, regulatory status, relevant regulations, and how they are being met. In addition, the procedure should describe operational processes that have been implemented to identify, prevent and mitigate the risks of money laundering and terrorist financing down to the level of operational deployment. Standard template policy and procedural documents are usually not acceptable. Rather, this must be tailored to a firm's specific business operations and the risks it is exposed to. Policies and procedures should be reviewed annually to ensure they are capturing new regulatory requirements.

A risk assessment describing an organization's risk exposure across several verticals. These should include geographical scope, products, services, delivery channels, client categories, partner types, new and emerging technologies, and other risks specific to a firm's business model. The risk assessment should detail risk mitigation measures in place for each of these verticals and a calculation of the inherent risk - risk levels before mitigating controls are implemented - and residual risk - risks that remain once mitigating controls have been implemented. The risk assessment should be up to date and be reviewed at least annually.

An effective **training program** is tailored to a firm's business activities and applies to all relevant staff in the organization who need to demonstrate competency and knowledge. This should include a methodology for training, a curriculum, documentation on training completion, and testing records. Training should be completed at least annually, and the curriculum should be updated regularly to address relevant regulatory changes and emerging financial crime trends.

Record keeping and reporting capture the operational activities relevant to the effective application of an AML compliance program, such as information on relevant regulatory bodies when parameters are met. Records to be kept include:

- Client files demonstrating customer due diligence has been completed at the stage of onboarding and periodically thereafter
- An up-to-date risk rating scoring for each client based on customer screening outcomes
- Documentation showing that transactions have been monitored t over the course of the business relationship with any client, including any that have been subject to a view

An effective **transaction monitoring program**, which should be automated rather than manual, is also a key determining factor. The solution used should be robust enough to catch internal issues, such as transactions indicative of financial crime, and external issues, such as a client's potential status as a Politically Exposed Person (PEP), a sanctioned individual or entity, or as being the subject of adverse or negative media. All of these functions must work in concert and must have been reviewed both internally by the compliance head and externally by a competent auditor (we will discuss this review requirement in detail in the last section).

Business Activities

Ensuring the business activities a firm offers are in the scope of the risk appetite of the banking service provider they are approaching is a key strategic decision for any organization. Many banking service providers are risk averse when it concerns certain activities offered by fintechs and MSBs. Some of the activities banks may decline to serve include check cashing, third-party access to accounts and services, serving high-risk jurisdictions, servicing privacy coins with respect to virtual currencies, and serving business clients with overly complex structures or obscured ultimate beneficial owners. When considering an application for banking services, it is important to discuss with the relationship manager prior to the application what business activities the prospective bank is comfortable with. Having a robust business plan, which describes the services offered and how they are delivered to customers, will be an integral part of a successful application.

Financial Fitness

The overall state of the applicant's financial health is another factor a potential banking partner will scrutinize. Profitability isn't essential - many firms will be operating with venture capital or other investments as backing - as long as the roadmap to profitability is realistic. The business plan documentation firms prepare needs to describe financial projections, profit/loss variables, and margins in detail. The assets-to-debt ratio will be closely scrutinized. The bank will also consider the depth of the financial ties which exist with any potential client, so firms should start by approaching banks they already do business with.

Legal Fitness

Unresolved litigation, liens, complex corporate structures, and hidden beneficial owners are factors that will severely limit a company's ability to secure a banking relationship. Firms should ensure their ownership structure is as transparent and straightforward as possible. Limiting exposure to offshore and fractional ownership is also recommended. Additionally, adverse media or mentions concerning fitness and probity listings will be difficult to surmount when establishing a relationship with a bank. Background checks and documentation on the suitability and experience of the executive team and the owners of a business will be an area of prime concern.

Audit Track Record

A strong record of both compliance effectiveness reviews and financial statement audits, commensurate with the age of the business, is a requirement of most institutions that offer services in this sector. The compliance program reviews will need to be completed at least every two years. The findings from the review will also need to be presented, as well as the measures taken to address and remediate any findings identified. Senior management sign-off on the completed review process is also a must. With respect to financial statement audits, the most recent report will be required during the application process. If one is not available, a notice to the reader document may suffice. The audit should back up the statements made in the business plan document and the ownership structure declarations. The audit will ideally have been conducted by a reputable and reasonably well-known firm.

Conclusions

If firms take away one key finding, it is the importance of continually reassessing and improving compliance systems. In addition, it's critical to an organization's internal success to ensure that its compliance systems align with overall business goals. While this list is not exhaustive, following these tips should help ensure firms have the best chance of accessing financial services. A checklist summary of the steps we've highlighted in this document are itemized below.

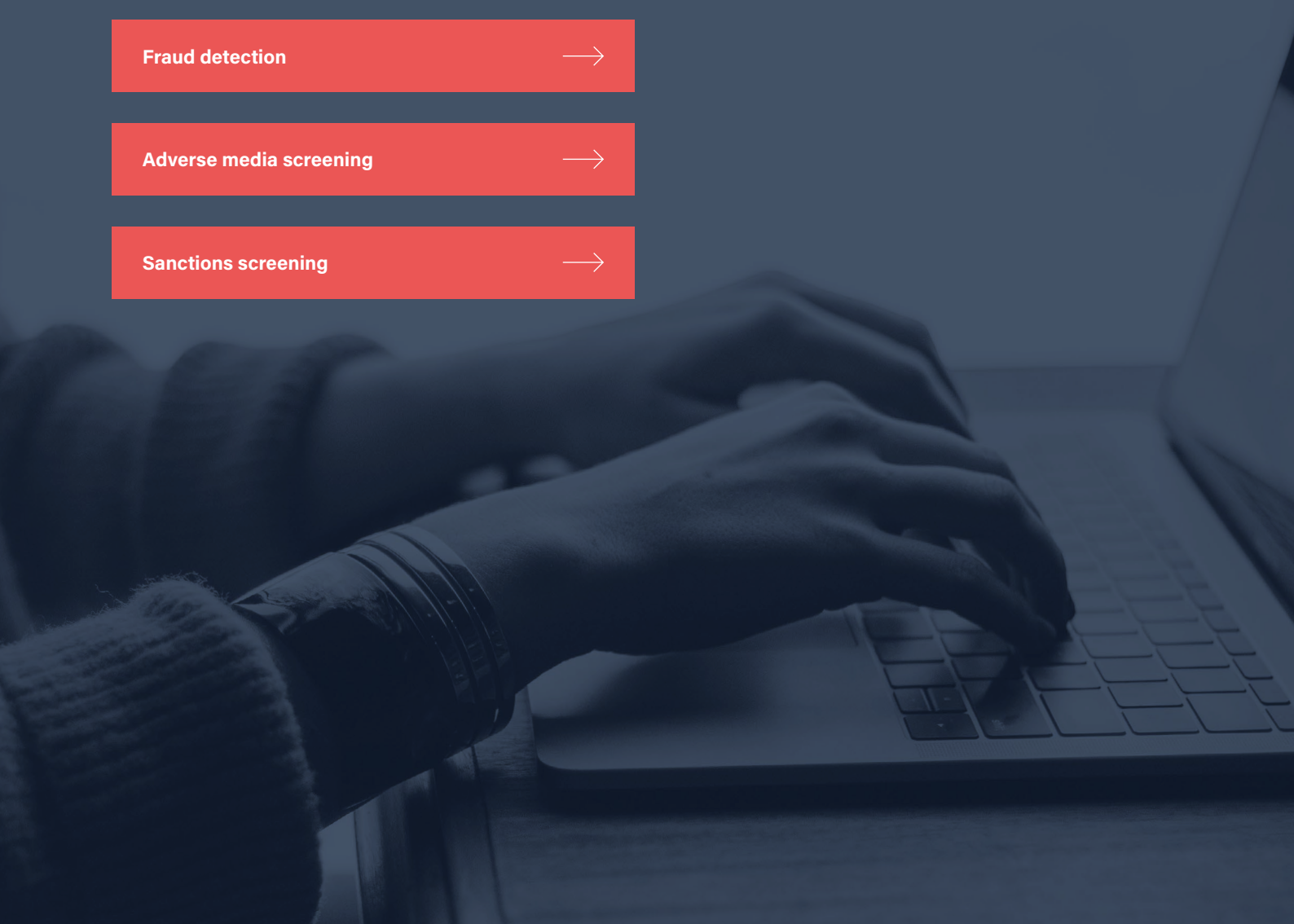
Compliance is a very complicated, rapidly evolving field requiring extreme diligence to succeed. Having automated compliance systems can help teams focus on the more important aspects of compliance, stopping financial crime in its tracks. If you have more questions about setting up a compliance system, ComplyAdvantage is here to help.

Next steps

If you're an early-stage startup looking for free access to award-winning AML and KYC tools, check out our ComplyLaunch program here.

Scale-up and enterprise firms can review our portfolio of financial crime risk detection solutions and book a meeting with our expert team using the links below:

- **Customer onboarding and screening** →
- **Transaction monitoring** →
- **Fraud detection** →
- **Adverse media screening** →
- **Sanctions screening** →



Checklist: Banking Application Requirements for MSBs

If you're a Money Service Business (MSB) or a fintech provider providing services similar to an MSB, accessing banking services can be a challenge.

That's why we've developed this checklist of the documents, procedures, and practices firms should have in place to maximize their chances of accessing the banking system. This checklist covers important topics such as compliance program completeness, business activities, financial fitness, legal fitness, audit track record, and more:

- ✔ Cover letter addressed to contact (champion at the bank)
- ✔ Appointment of a qualified Head of Compliance
  - » Resume
  - » Appointment documentation approved by senior management
- ✔ AML policies and procedures tailored to operations
- ✔ Risk assessment
- ✔ Training program
  - » Training policy
  - » Training materials
  - » Records of training outcomes
- ✔ Record keeping
  - » Client file for each client containing KYC
- ✔ Transaction monitoring system
- ✔ A sound process for submitting reports to regulators
- ✔ A business plan document outlining current and future business activities
- ✔ Audited financial statements, or other evidence of a sound financial position
- ✔ Ownership structure document and chart
- ✔ Declaration confirming the firm is not involved in any lawsuits, liens etc.
- ✔ Last compliance effectiveness review report
  - » Confirmation all findings have been addressed
  - » Management sign off
- ✔ Most recent regulatory audit report
  - » Confirmation all findings have been addressed