Building an effective AML framework for the fintech industry

REFINITIV

An LSEG Business

Source: White paper - How fintechs can address AML challenges

New technologies and industry-wide digitalisation are enabling better solutions across the sector – from payment processing, digital banking and crypto exchanges to insurance, lending, wealth management and more.

Given the many challenges that define the anti-money laundering (AML) landscape, companies need to build resilient and effective compliance frameworks.

Five core elements of such a framework include:

1. CUSTOMER ONBOARDING

Effective customer screening, KYC and enhanced due diligence when required are the key pillars of successful customer onboarding, but ensuring a positive customer experience remains absolutely vital.

Digital onboarding transforms time-consuming, paper-based onboarding processes and replaces them with dynamic, client-friendly experiences that also boost efficiency and save time. It is important to bear in mind that all

Questions to consider:

- Can the technology we employ identify fraudulent documents?
- Can it confirm that the person trying to transact is alive?
- Can it uncover adverse media risks?
- Can all of these activities be completed in real time?
- Can all of this information be collated for back-end systems to consume?
- Can I identify the risks that are associated with the entity that I am onboarding?
- Can I identify whom I am doing business with?
- Can I verify the person I am doing business with is who they say they are?

2. ONGOING MONITORING

AML obligations extend well beyond initial onboarding. Monitoring ongoing customer behaviour is also crucial, since red flags can emerge at any stage and ongoing checks are necessary to assess this changing risk.

Questions to consider:

- Are we getting the right alerts from our screening dataset?
- If yes, how are these alerts manifested in our overall customer record?

3. TRANSACTION MONITORING

Transactions should be monitored for any red flags. For example, if a customer is sending payments to an entity that is either directly or indirectly sanctioned.

Questions to consider:

- Is any customer vulnerable to a fraudster?
- Are any accounts showing warning signs of account takeover?

4. CHANGING CIRCUMSTANCES

Monitoring for changing circumstances is a form of perpetual KYC. Financial firms must remain mindful of which data points should trigger a new KYC process. There are various factors to consider here, including the weighting given to specific data points, the initial risk score generated and other relevant factors.

Questions to consider:

- Is our current onboarding tool helping us to monitor for changing circumstances?
- If an address change triggers an ID verification process (for example revalidating the name and address against an official data source), does our current system request an ID stating the new address, followed by a liveness check?

5. RISK SCORING

There are several factors that contribute to a customer risk score. It is important to ensure that all information captured is collated and that each system used has a machine-consumable result set that can be fed into the risk engine on a continuous basis, helping to ensure that the customer experience is consistent with any possible risk tagged against them.

Questions to consider:

- Are they who they say they are?
- Will they cause you legal risk or damage your reputation?
- Will they cause you financial harm?

Click here to learn more about more about **our AML solutions for fintech**.

Visit **refinitiv.com** | @Refinitiv Refinitiv

REFE/K20200109-22

REFINITIV

An LSEG Business