First AML

WHITEPAPER

The Fintech Frankenstein Dilemma

Navigating Compliance Challenges and Scaling Safely.

Introduction

"Move fast and break things" is the mantra of the fintech explosion over the last 15 years. But as the industry matures, and governments come to grips with regulating the sector, the mantra is at odds with the changing regulatory landscape.

Fintechs are now expected to "move fast & scale things". We're seeing unscalable compliance hindering the scale of these businesses across the globe, with significant de-banking examples, regulatory clamp downs and sharp drops in share price overnight on accusations of money laundering.

This paper will go into some of the common mistakes fintechs make when setting up their compliance functions, the relationship between UI/UX & compliance, and the new wave of regulation technology helping firms do compliance at scale.

We will also look at the optimal new KYC model that fintechs of all sizes (from start-ups to scale-ups) are using to future proof their compliance.

The cost of getting this wrong.

The cost of getting compliance wrong for fintechs has never been greater.

As U.S. Attorney General Merrick Garland stated, “Using new technology to break the law does not make you a disruptor, it makes you a criminal.”

This comment was made in relation to Binance, which has recently pled guilty to facilitating money laundering and terrorist financing. Due to resulting regulatory pressures, Binance has exited multiple markets, paid $4 billion in U.S. fines, and seen its CEO resign while facing potential jail time and personal fines.

Binance is not the only high profile fintech to be adversely affected by AML issues.

Earlier in 2023, Block and its most profitable product ‘cash-app’ was accused by Hindenburg research of being the go-to-app for money launderers, gangs and rappers in the US, causing a 35% drop in their share price in one day and wiping billions off their share price.

The impacts aren’t always regulatory. Recently the popular B2B payments and banking provider Wise stopped B2B onboarding due to significant volume increases and issues with letting sanctioned individuals make transfers (of which they are still investigating). They are receiving unprecedented demand but are having to pause customer onboarding, which is the last thing you want to be doing as a fast scaling fintech.

All of the above examples have one thing in common: a scalable front-end user interface, with a focus on new customer onboarding, while lacking the back-end infrastructure to scale their compliance effectively.

The typical KYC Stack.

The allure of pointions

Fintechs are often drawn to front-end focused identity verification and biometric solutions for their slick user interfaces and perception that KYC is a one-time process rather than something requiring ongoing monitoring and infrastructure. The appeal is understandable - who wouldn't want a smooth onboarding flow for customer?

This however, as firms quickly realise, is only one piece of a multi-dimensional puzzle when it comes to their AML obligations. While the front-end customer experience is crucial, many firms overlook the need for robust back-end infrastructure to store data, handle escalations, and enable long-term scaling. Without structured processes on the back-end, processes quickly become un-scalable and prone to breaking. While the front-end dazzles, the back-end infrastructure crumbles.

Challenges encountered by product and operations teams

Typically in an early-stage fintech, the individuals involved in building the onboarding process are product and operations professionals who may lack a deep understanding of AML requirements and workflows.

Building (from scratch) and maintaining such a system can be difficult, especially for early fintechs focusing on customer-facing aspects rather than the less exciting but crucial back-end infrastructure. The lack of attention to these backend elements can contribute to a system that is ineffective at best, non-compliant at worst.

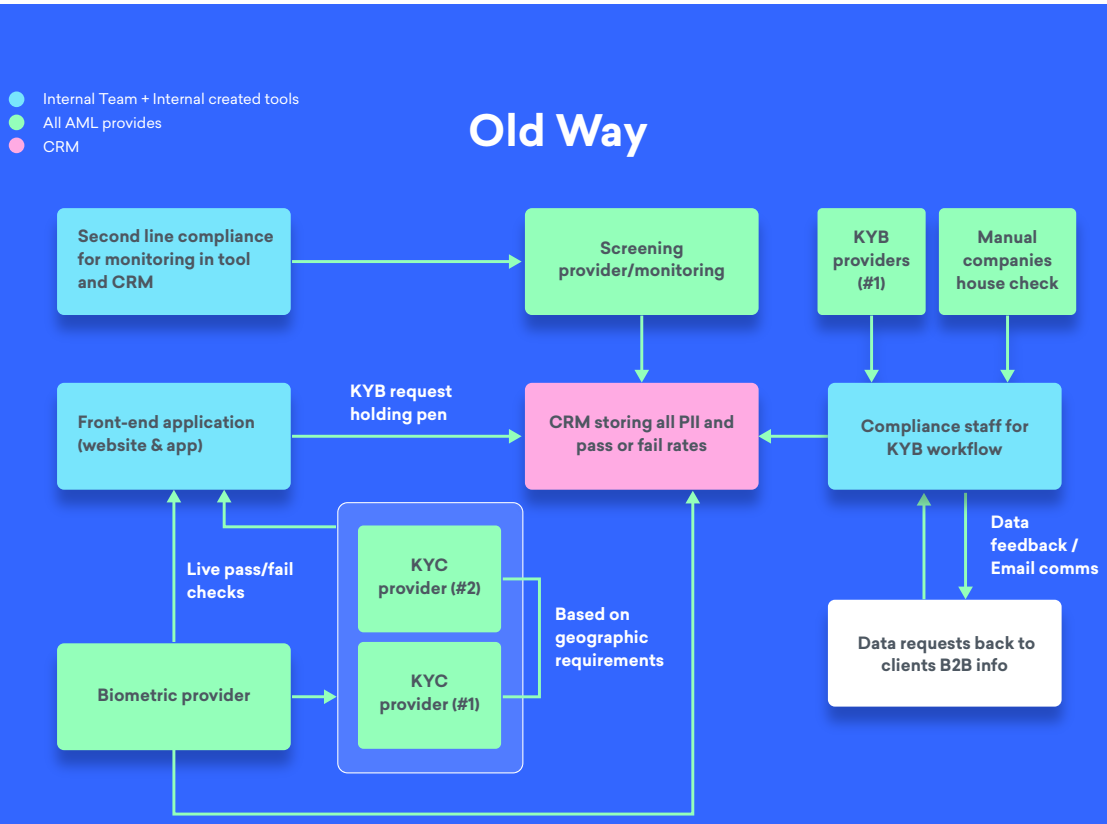
What's more the integration of multiple point solutions comes with a high cost and complexity. As an early fintech, predicting flow might be difficult, making it difficult to negotiate volume discounts and leading to potential overpayment for services. Vendors may also attempt to lock businesses into onerous contracts, adding further challenges.

It's not just about user experience

Quickly integrating a verification vendor without sufficient thought for what happens afterwards is a common misstep. User experience is important, but how customer data and documents are handled after initial collection is just as critical.

As time passes, fintechs often find themselves in a frantic pursuit of additional tools to address various facets of the AML puzzle, including sanction screening, ongoing monitoring, PEP, anti-fraud, and KYB solutions.

This typically involves a CRM at the proverbial heart of this newly created AML version of Frankenstein's monster. What was sold as a scalable way to onboard clients, turns very quickly into an unscalable way to keep track of the clients when onboarded, with sensitive PII data held in CRM cloud tools.



In response to this scenario, many fintechs find themselves entangled in the process of disentangling between 3 to 7 tools, each with varying contract lengths and addressing different aspects of the AML problem. This predicament poses a significant financial burden for businesses, creating a substantial sunk cost challenge, especially for those unable to pause their customer onboarding operations, even for a brief period.

Leaving revenue on the table

The way these solutions are often implemented do not allow customers to sign up without passing these checks automatically which also leaves a lot of revenue for fintechs on the table, with a few adjustments to the operating model, having an orchestration layer to deal with failed cases could see failure rates reduce by 7-9%.

If anyone has non-English characters in their name, or used a foreign passport to try to sign up for a digital bank or other fintech solution will know the pain well. The AML Frankenstein has no tolerance for this sort of onboarding with too much resource required to remediate or override these sorts of cases.

The AML Frankenstein isn't the fault of the fintechs – it affects almost every industry that has AML requirements. Historical solutions are expensive and clunky and the new wave of regtech solutions have started 'narrow' in their offerings, whereas the sector requires broader, more complete solutions. This is a big criticism of a lot of tech solutions in general, narrow solutions solving narrow problems, whilst this works ok in a lot of industries, the regtech space, requires more holistic approaches to allow businesses to scale properly.

The sector requires broader, more complete solutions.

Common issues in the KYC data lifecycle.

There are broadly two stages of maturity that we see in the market for fintechs. The first stage fails to deliver the flexibility and value that fintechs now need to compete effectively, mitigate risks and build commercial resilience.

- **Model 1 - point solutions**
  Organisations implement point solutions to solve narrow problems.
- **Model 2 - holistic KYC**
  Automation and integration by default and data is considered within a broader, multi-functional and longer term view.

When the first model meets common scenarios, the limitations of the piecemeal approach, visualised further below, are quickly exposed.

Common scenario 1:

When electronic identity verification (eIDV) fails

This leads to failure without remediation, and a frustrating customer experience.

- The failed ID checks are stopped at the customer side, for reasons as varied as blurry photos, false PEPs, or mistyped information
- If a back up process is available it requires customers sharing additional information manually.

When information is collected via scanning, photo or PDF, the data contained within is unstructured and unable to be consumed back into the system of record without manual handling.

Data is then manually keyed in, or copied and pasted, and is often double or triple handled to enter into multiple systems.

This non-digital process means that useful metadata that could be used to drive future AML workflows such as ongoing customer due diligence (OCDD) is unable to be captured.

Common scenario 2:

Onboarding a business customer owned by a trust or overseas shareholder.

- The application is taken, an entity structure is built out, but once a trust or overseas shareholder is identified the process stops.
- Many KYB providers can't go beyond the simplest of entity structures to identify ultimate beneficial owners (UBOs) or verify overseas shareholders.
- Much like the eIDV failure, front line employees are then tasked with manually collecting source documents (such as trust deeds), exposing the organisation to further data security and privacy risk.
- After much back and forth (and associated inefficiencies) the documentation is received and the process starts again.

Common scenario 3:

Excessive false positives associated with PEPs and sanctions checks.

Much like scenario 1 of an eIDV failure, false positives create cascading inefficiencies.

- The flagged match sits in a queue waiting to be reviewed. Time elapses.
- Once at the top of the queue, back office employees are tasked with manual investigation.
- If it's a common name, such as John Smith or Zhang Wei, the manual search to cross match against birth date or another unique identifier, takes even longer. More time elapses.
- Eventually a match decision will be made and the process starts again.

Scaling compliance correctly: the rise of AML orchestration.

AML orchestration describes best-in-class, configurable workflow solutions in which combine multiple point solutions into one, holistic customer onboarding platform. It combines the slick customer-facing biometric experience that fintechs obsess over with heavy-hitting compliance providers in the PEP/sanction space, as well as KYC registers and global data sources, into one scalable platform.

Think of it like a specialised end to end tool for compliance which clips onto an existing full CRM. A great example of technology like this in other sectors are firms like Outreach.io, and Salesloft which are specialised out of the box outbound selling tools which are then integrated into CRMs like Salesforce and Hubspot. The rise of these tools have replaced archaic self-built workflows within CRMs themselves, which, if not designed and architected properly, become an extreme burden on the users of the workflows.

Tools that build in this space understand that organisations want the best version of the workflow and most efficient way to handle the breadth of their AML obligations. The organisation's desire was never to design and build their own system. The custom built - workflow simply arose out of a lack of other options.

However, creating a custom-built workflow introduces the next challenge – organisations often design these workflows with a lack of understanding, either in technology or AML requirements. The absence of a deep intertwining of both elements hampers the system's scalability.

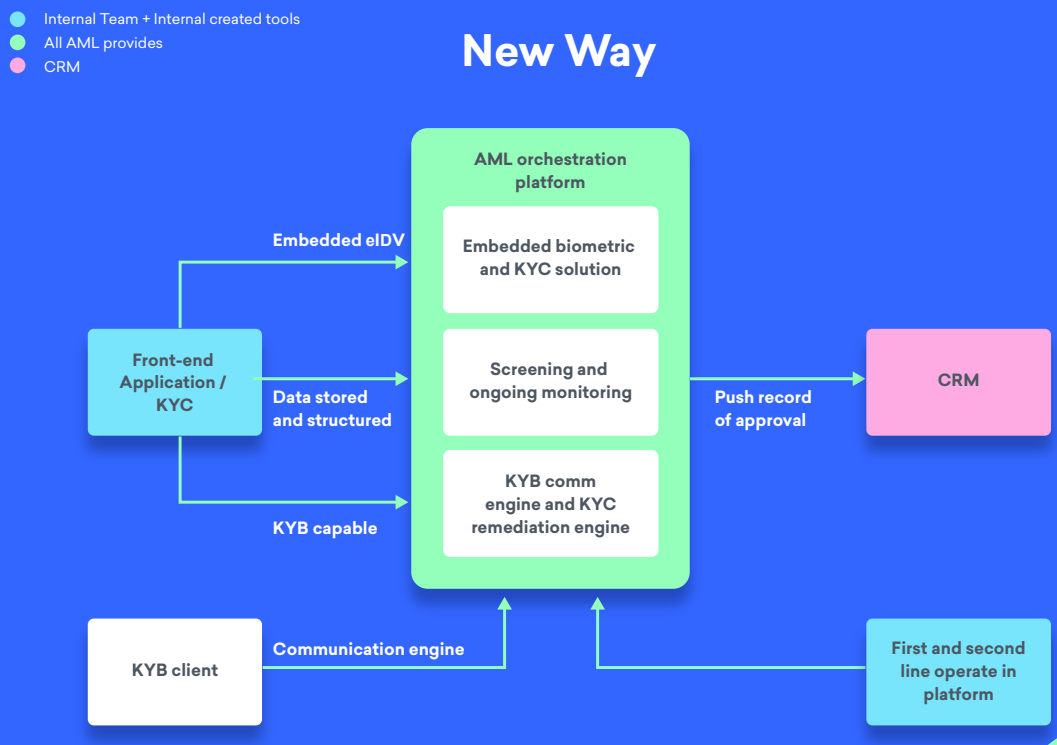
To build an effective orchestration platform, a mix of skills encompassing a deep understanding of technology and compliance is essential. Collaborating with orchestration platforms experienced in working with compliance teams provides a significant advantage when establishing a scalable system.

Custom configuration versus custom-built workflow

When searching for an AML orchestration platform, another crucial feature is custom configuration, enabling in-platform adjustments for KYC and AML processes based on jurisdictional requirements and company-specific risk factors, without the need for the extensive internal resource allocation required for building custom workflows across existing point solutions.

Picture a set of train tracks — a custom-built workflow involves constructing entirely new tracks to reach a new city, while custom configuration is akin to using a railroad switch to redirect the journey toward the desired destination. AML orchestration platforms leverage built-in infrastructure that can be adjusted, as opposed to constructing entirely new, inflexible tracks that become obsolete after use.

Previously, purpose-specific custom-built workflows demanded technical resources for any alterations. With custom configuration, adjustments can be swiftly implemented in the system as required—whether due to regulatory shifts or internal risk changes—and can be overseen by a non-technical MLRO.



Conclusion

It's clear that AML/KYC technology offers transformative potential by enhancing efficiency, scalability, risk reduction, and regulatory compliance.

This guide has outlined essential concepts to buying and implementing the right AML technology into your company's onboarding process.

What we're seeing in fintechs that are nimble, profitable and compliant, is a new approach to data governance. Data is considered in a broader, more agile context, moving from siloed one-time use cases to a wider, longer term approach.

As Saul Judah, VP, Data and Analytics, at Gartner notes, "Due to varying levels of uncertainty in today's world, data governance needs to embrace speed and agility, which has rendered traditional approaches ... obsolete."

This agile approach sees data as a strategic asset that can help:

- deliver superior customer experiences.
- mitigate a broad array of risk; and
- maximise operational efficiencies.

Establishing a scalable orchestration platform from Day 1 is the future for fintech onboarding. There's no doubt that current processes leave much to be desired, and as the regtech market matures, an increasing number of firms will gravitate towards AML orchestration, moving away from narrow solutions that are becoming increasingly commoditised.

The collaboration between technology experts and regulatory experts is essential. Each needs to understand the limitations of the other, and only through a collaborative understanding can they create effective orchestration layers for fintech.

About First AML

This paper is not only written from the perspective of a technology provider, but also from the lens of compliance professionals. Prior to releasing Source, First AML's orchestration platform, we processed over 2,000,000 AML cases ourselves. Understanding the acute problem that faces firms these days as they try to scale their own AML, is in our DNA.

First AML powers thousands of compliance experts around the globe to reduce the time and cost burden of complex and international entity KYC. Its enterprise-wide, long term approach to the CDD data lifecycle addresses time and cost challenges while improving the customer experience and minimising reputational and security risks.

First AML