



AML RegTech
Vincent White

The recent report commissioned by the City of London Corporation delivered a stark clarion call to press forward with the adoption of RegTech, not merely on the grounds of incremental efficiency improvement, but to embrace the suffusion of technology within the compliance sector as a paradigm shift, and an integral part of digital transformation. The scope of the research included a vendor survey and consultations, and qualitative interviews with financial institutions and regulators.

As with the emergence and adoption of any new technology there is the perennial problem of 'alignment' to achieve greater uptake, underpinned by mutually beneficial outcomes. From the perspective of financial institutions, this may mean separating the wheat from the chaff among vendors, lifting the lid to distinguish the genuinely valuable from the bells and whistles; and by extension, expecting vendors to improve awareness and understanding of their pain points such that solutions are fit for purpose, and to that end, their benefits can be articulated and evidenced.

From the vendor point of view, there are the more prosaic, practical obstacles, such as protracted procurement cycles, particularly of large institutions, and the product 'stickiness' of existing, embedded systems, possibly compounded by an aversion to new technology as being inherently risky. Lengthy procurement processes are nothing new, but they do have a greater impact for services based on fast-changing technology. Vendors may also echo the view that financial institutions may lack awareness of the benefits RegTech can bring.

Regulators may recognise their advocacy role as a catalyst for adoption, but equally are constrained by the need to be 'market-neutral'. They assert their support for technology innovation, as attested to by numerous innovation initiatives, programmes, and pilots - but will not be drawn to drive or lead this change, as the Bank of England Deputy Governor Sam Woods said at a launch event for the report. Noteworthy is that technology adoption is still not an element of supervisory discussions with regulation firms.

Key findings in the report highlighted that vendors see this as a role of the regulator, to encourage RegTech adoption, that this the most critical driver for growth.

It is debatable why the general support of innovation by regulators while maintaining neutrality has not been successful, given other contexts where this is the case, for example, in recent FATF mutual evaluation reports that have encouraged technology adoption. However, the report includes in its recommendations the suggestion that it may not be possible to maintain neutrality with the accelerated pace of digital transformation.

Within the taxonomy of RegTech, financial crime compliance is one area that stands to benefit hugely from adoption new technology, and the principle reason for that lies in its data characteristics – the territory of KYC and AML often comprises both 'big' data, and an overall process that has adopted automation relatively early, but suffers from bottlenecks that undermine operational efficiency.

Processes are already highly automated in some areas – and they need to be – transaction monitoring being a case in point. Within watchlist screening, data cleaning and collation, batch screening, ongoing monitoring, and exception handling are all large-scale, complex processes, but are now largely software-

driven. But match resolution itself remains a manual process, necessarily requiring human oversight and judgment. We would not wish to ‘design the pilot out of the cockpit’ so to speak, but this particular bottleneck is caused by the shortcomings of alphanumeric matching systems, the inherent characteristics of names, and the predominant labels used to identify entities.

A matching system based on biometrics overcomes the linguistic obstacles, and addresses the problems that arise in identification, not least, identity fraud.

The main pillar of data delivery is now the API, as in the adaptation to open banking, serves to provide a tranche of advances that can be measured in terms of efficiency, but also in simplification and effectiveness.

Accelerating onboarding and deepening data integration

KYC makes up a significant portion of AML budgets, up to 40-50% in some cases, and the composition of that spend is largely manpower rather than technology – it’s a very labour-intensive process.

Much effort is spent collecting information, screening names against lists or adverse media, and going through results. Many of those processes are manual and compliance teams need ever larger headcounts to process and resolve alerts. The application of biometrics is one example where this tail-end bottleneck can be radically transformed.

In addition, there are the indirect and less visible costs: the increasing time spent to onboard new clients, days or even weeks in some cases, leads to a poor customer experience, friction, frustration, and many applications are abandoned – this has a negative impact on the client lifetime value as well as significant revenue loss.

APIs have allowed risk data to be collated, standardised, and centralised, linking different elements of KYC processes, e.g., ID verification, UBO identification, and corporate data. Deeper integration moves away from disparate siloed or disconnected solutions and delivers further efficiency improvement.

Digital Transformation and Automation

Transactional behaviour should already be linked to customer data, but separation between systems can hamper the single view of customer. Customer data may be distributed functionally, by product or department, in addition to consolidating the elements of KYC that have a bearing on risk, into a unified view in real time, rather than staggered updates between systems. AML data should also be linked into CLM/CRM systems.

Above all, APIs offer a means to support further digitalisation, and the transition away from laborious, manual tasks that are ripe for automation. As an increasing number of systems and processes become digitalised they, in effect, achieve a critical mass that facilitates the customisation of infrastructure, giving greater flexibility and transparency, such that institutions can mould their internal architecture using the building blocks of various APIs.

The relentless pace of advancing technology, commonly expressed as a variant of Moore’s law, with exponential growth in many areas that technology touches, means that the digital environment experiences an ever-ascending ceiling of technical limits – what is not possible today due to, for example, processing, memory or bandwidth constraints, will likely soon be possible on the near horizon. The upshot is that APIs can now comfortably accommodate rich, biometric data – which inherently contains more information – affording the possibility of using an underlying data type that is inherently superior to alphanumeric data in the context of AML/KYC, as it delivers better performance in terms of accuracy, efficiency, and effectiveness.