A1LoD report®

Re-defining know your customer

FORECAST 2022

Part of the Financial Crime Roundtable report series

Commissioned by: quantexa

Re-defining know your customer

The traditional know your customer, or KYC, process is changing. The core customer due diligence (CDD) and enhanced due diligence (EDD) processes – which are based on periodic snapshots of client data, driven by specific regulations – will need to provide a more continuous, risk-based review of individual and corporate clients in future. And as regulators demand more information about the holistic financial crime risk of clients, rather than simply wanting to see the right data and documentation, banks will have to deploy new technology to spot patterns and activities that are invisible to the human eye.

Most financial crime professionals agree that the KYC/CDD process is the foundation of effective financial crime prevention. Without a deep knowledge and understanding of who their clients are, their ownership and relationships with other entities, their normal behaviour patterns and any deviations from the norm, and how those clients may change over time, it is impossible to build up a satisfactory picture of the financial crime risk of a particular client. Not only does that expose banks to unknown levels of risk, it also prevents them from aligning any risks that they do take with a defined risk appetite. KYC/CDD is also, by definition, the foundation for sanctions, anti-bribery and corruption (ABC) policies, and other anti-money laundering (AML) activities.

The standard criticism of KYC/CDD processes is that they are point-in-time. Whether this is at the point of bringing a new client on board, or during an EDD escalation or a periodic review, even if it is event-driven, banks are really only looking at clients in snapshots. There are other issues too. The processes rely too much on data supplied by the client (which may be late and partial), on external sources of information (which may be inaccurate), and on adverse media screening. All of these processes can throw up far too many false positives.

One solution to these problems is to adopt a more continuous version of KYC, using a smarter analysis of the data that banks already have at their disposal. This could include: transaction data from anywhere in the commercial or investment bank, or from the wealth management business; payment data; information on borrowings and related-party transactions; and additional, third-party sources.

This strategy of perpetual KYC leads inevitably to discussions about data, analytics, dashboards and technology in general. But at 1LoD's latest KYC leadership discussion, it became clear that for many institutions, particularly the larger regional or global banks, another set of issues must be addressed first.

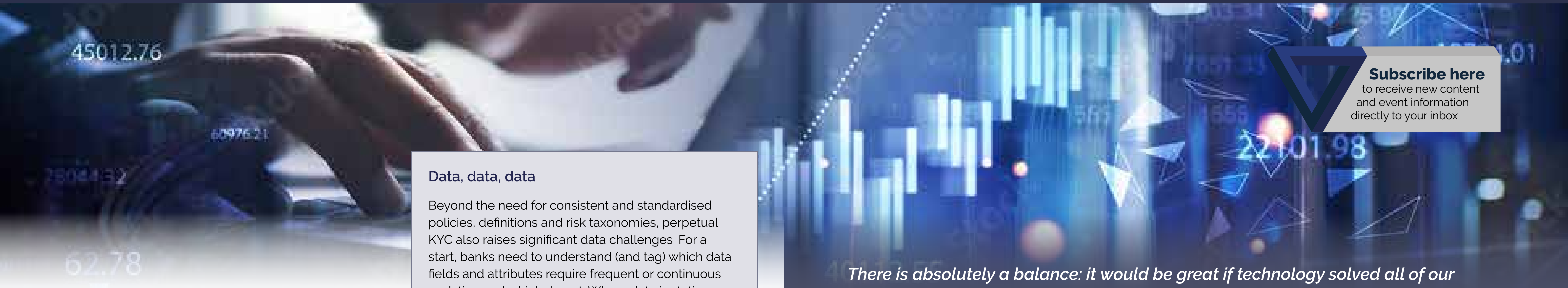
Policies first, technology second?

The first is organisational and regulatory. Banks have numerous different franchises, regional and country businesses, and legal entities, each with their own standards, policies and risk ratings. At their core, these are driven by the different regulatory standards applied to different types of organisation in each jurisdiction.

But this regulatory fragmentation is exacerbated because of the way that KYC/CDD is operated differently by different business divisions. For example, one participant explained how their bank has "one financial crime policy and then, underneath that, core standards – one for sanctions, one for ABC, one for CDD – but then around 20 different sub-standards underneath that depending on where you are in the bank. These businesses also risk-weight differently, they review relationships differently and at different times, and so all our legal entities and franchises are singing from different hymn sheets, reaching out to the same client, asking for different things because they have different CDD processes."

So, before they can even think about deploying new technology, many banks are working on foundational programmes to, for example, group clients across the various business lines, investment bank, and corporate bank, in order to avoid multiple outreaches and gain efficiencies. In many cases this means consolidating highly manual processes.

For example, the creation of a common CDD standard is, at its core, the creation of a hierarchy of requirements that become 'live' depending on the jurisdictions and products and legal entities involved in a particular client interaction. So, clients might be grouped for refresh according to the strictest jurisdiction in which they operate, or according to the highest risk category demanded by a region. Some banks have developed in-house regulatory technology, or regtech, tools that activate the relevant fields depending on whether particular product or country boxes are ticked, but many are still creating these hierarchies manually.



"Right now, we are consolidating documents and spreadsheets," says one top-tier US investment bank. "The way we originally had it is you have one global policy and then each region has their own policy. So, you could have up to 26 different regional KYC standards – up to 26 different checklists that have data and docs associated with them. And we are now consolidating that into one standard, one checklist."

The frequent lack of a single policy and taxonomy also causes problems in knowing what qualifies for KYC and what does not. "There may be parties in your reference data system that don't require KYC," one 1st line KYC head explains. "So, the first step of efficiency is carving those out and then applying those resolution standards to the ones that require KYC, limiting your resources to those entities."

For many financial crime professionals, these kinds of problems militate against a straightforward technology solution. "It's not just about the technology you need," says one financial crime professional. "You really need to make sure that you've got that single CDD standard that meets all regulatory requirements in different locations, as well as the technology to back that up. The true challenge of KYC is to be able to do it across multiple countries with multiple operating models and multiple requirements."

Vendors agree. Clark Frogley, head of financial crime solutions at Quantexa, has spent much of his career working for bulge-bracket firms. He says: "There is absolutely a balance: it would be great if technology solved all of our problems, but technology has to marry with the policy and the operational issues and the regulatory issues. They all need to come together. That said, technology has advanced and what we can do now with the data was not possible just a few years ago. So, one way to start is just to ask, 'where's my low-hanging fruit? What can I begin to monitor today? How do I begin to solve for some of those key challenges?"

Data, data, data

Beyond the need for consistent and standardised policies, definitions and risk taxonomies, perpetual KYC also raises significant data challenges. For a start, banks need to understand (and tag) which data fields and attributes require frequent or continuous updating and which do not. Where data is static or only periodically reviewed, it should stay that way and only the data that contributes most significantly to changes in the true risk score of a client needs to be updated more frequently.

Designing that tagging exercise and making it universally applicable is an important next step in moving from, for example, annual reviews with EDD triggers to a more event-driven overall review process, to a fully perpetual model. In a sense it is an extension of some of the ongoing screening processes already carried out in KYC/CDD/EDD functions. Banks need to work out how to take that mechanism and apply it to the other attributes that make up KYC.

Changes probably also need to be made to the business practices that support such a continuous KYC process. Institutions receive client data regularly via different business divisions when clients buy products and use various services. That data is frequently "structured in a way that doesn't complement how you want to do KYC, and if that is the case, then you're perpetually going to be in remediation," says one financial crime managing director. "You have to have business practices that support what you're doing in KYC. And that requires a business practice change around data standards and policy standards that allow cleanliness to be retained. We can't be perpetually cleaning this data up."

More broadly, aligning KYC with the business is crucial. The 1st and 2nd lines, as well as external partners, must ensure that accountability in the business is very clear. As one bank just out of remediation puts it, "We are building out a culture where my organisation [KYC operations] feels that they work in the KYC space for a business, but within a [bank-wide] standardised framework. The better we align with the business, the faster files are removed."

There is absolutely a balance: it would be great if technology solved all of our problems, but technology has to marry with the policy and the operational issues and the regulatory issues. They all need to come together. That said, technology has advanced and what we can do now with the data was not possible just a few years ago. So, one way to start is just to ask, 'where's my low-hanging fruit? What can I begin to monitor today? How do I begin to solve for some of those key challenges?

Know your customer, really

Solving the issues described so far is crucial. There are technology aids for most of those problems, including regulatory technology platforms, workflow solutions, data cleaning and aggregation software. However, some of the most significant inherent risk in the KYC process cannot be mitigated simply by increasing the frequency of regulator-mandated reviews, nor by the continuous review of currently required data fields that have been identified as 'dynamic' rather than 'static', such as adverse media hits or ownership changes etc.

The regulators recognise this and have started to ask more searching questions related to risk. They take the core, box-ticking regulatory minima for granted, according to one financial crime veteran, and now "they are asking analysts to take a step back and to look at the financial crime risk of that client and what its connections and transactions tell you about that risk, not what is simply written down on the pieces of paper that we have to gather for standard KYC. The regulatory expectations have gone to a whole new level."

The only way to evaluate risk in that way is to look at ongoing client behaviour across all the data available within the bank. This includes transaction and trade data, data gathered for the purpose of making credit decisions, payment data, ABC- and sanctions-monitoring data and so on. It also means banks must truly understand their clients even when those clients are complex and opaque in structure – and where legitimate (and illegitimate) obfuscation make it essential to work out relationships.

To take the example of transaction monitoring, or TM, clients who are repeatedly highlighted by current, unintelligent TM alert systems could be reported back into a continuous KYC process and have their risk score increased. More significantly, smart, AI-driven, pattern-recognition software which is run over that same transaction data is already able to identify true positives far more accurately, making that basic feedback mechanism much more effective. Some versions can also reveal suspicious trading or payment activity and can even detect hidden entity relationships from huge datasets, whereas human analysts would find it impossible to unearth such information unless the banks involved increased the level of manpower significantly to hundreds or even thousands of reviewers.

This is a truly risk-based, continuous, review of customer behaviour, and it clearly has the potential to enhance any periodic or continuous review process. However, it is not a conventional definition of KYC. KYC today refers to the onboarding process. It is some form of more-or-less frequent periodic review of data points largely determined by regulatory norms and it is an enhanced due diligence process for clients defined as high-risk according to the banks' own risk

scoring systems. As one KYC head says, “That is talking about account activity screening, rather than actual KYC.”

Even comprehensive entity resolution – the application of one market standard identifier for a client and all their related parties that is available across all businesses and markets – is not viewed as a standard part of the KYC process. Typically, banks keep separate files even for related entities for reasons of simplicity and do not have processes for linking them systematically.

That said, leading bank are using these smart analytics and pattern-recognition systems to improve their financial crime and AML risk management. But they are doing so via transaction monitoring. One bank which has been running Quantexa as a replacement for the standard TM system for two years describes the difference between the quality of the alerting as “night and day. False positives are dramatically down and true positives that lead to SARs (suspicious activity reports) are up significantly and the linkages being revealed are incredible, so we've got a much better view of the financial crime risk versus a KYC analyst with just a point-in-time view of a client or a TM analyst just looking at transactions in isolation.” And with AML fines running into the hundreds of millions of dollars, the $5 million to $10 million price tag for some of these new technologies appears reasonably good value.

As well as the obvious risk management benefits, installing the system has allowed this particular bank to transform its TM analysts team into a more highly skilled, investigative operation as well as revealing multiple opportunities for cross-selling and upselling clients. The financial crime head behind the programme explains, “we're selling it internally on the basis of the commercial angle, not ‘sorry, financial crime want more money again’. This is smart information that the business can use to their benefit as well as improving the control environment from a fin crime perspective.”

This move is just a first step. Today these systems overlay TM and solve a more general AML problem, rather than a standard KYC problem. The analytics can help to build the holistic picture that regulators are starting to demand from banks, but the next stage is to feed these new TM insights back into the true KYC review process as real-time data that helps to drive risk-scoring and escalation. For now, that is a goal or ambition, not least because, as this banker says, “the TM teams are very separate to the KYC teams. They're under different leadership. Systems just don't speak to each other in the way that they need to.”

True next-generation KYC will incorporate this data into continuous reviews that should, in time, replace periodic CDD. Whether or not it affects EDD is moot: there will always be a place for an escalation process triggered by a risk event, and these new analytics systems may create more of those events. But as Frogley of Quantexa says, “It's hard to overstate the importance of truly knowing your customer to everything we do in financial crime. If we want to make a real difference to the incidence of financial crime then we need to bring all the data we have at our disposal together – from TM, ABC, sanctions, wherever, And the technology exists to bring that data together more effectively and to utilise it in ways that have simply not been possible before.”