SHIFTING GEARS!

THE PATH TOWARDS NEXT GENERATION TRANSACTION AND COUNTERPARTY SCREENING

Vision Paper
October 2020

For many years, Transaction and Counterparty Screening has been a regulatory expectation in most countries as part of the broader Anti Money Laundering (AML) and Counter Terrorist Financing (CTF) regulations. It applies to all financial institutions but also increasingly to fintechs and corporates, which – beyond the compliance expected by their local authorities or their banking partners – also rightfully aim at making a positive ethical contribution to the whole community by helping fight financial crime.

To that end, financial institutions - and also more recently fintechs and corporates - have implemented many processes, policies and controls to cope with increasingly complex and far-reaching regulations as well as financial crime schemes. Non-compliant organisations have received heavy fines which often had not only a strong impact on their bottom-line but also on their reputation and their ability to operate in specific markets, segments or products. Compliance resources have also grown considerably within those organisations, with teams of several thousands of people now being the norm for large financial institutions. According to recent Celent estimates, the financial community spends around 30 billion USD every year at global level to fight financial crime.

And yet, the outcome is still really disappointing. It is estimated that only 1% of financial crime is actually prevented. While there is no doubt about the commitment of all players involved and while a lot of money is being spent, we should face the reality: we are currently collectively dramatically failing in our fight against financial crime. And to make it worse, the heavy compliance processes have also significantly undermined both the quality of the service being offered to end users and the pace of market innovation.

Time has come for a major change. And the good news is that almost all the enablers are now in place to make it happen. A number of new technologies can now be leveraged. There is also a genuine desire within the community to collaborate and the emergence of the first utilities has shown the positive potential impact of such collaboration. And finally, there is progress being made on data sharing, a sensitive topic that can be instrumental in the effectiveness of the fight against financial crime.

This paper successively covers the need for change in the transaction and counterparty screening area, the new technologies that can be leveraged, the emergence of utilities and finally the data sharing opportunities.

Status quo **is not an option**

The current approach toward transaction and Know-Your-Customer (or more generally counterparty) screening is not sustainable:

a) **Low efficiency**. The processes and technologies currently used by financial institutions result in very low efficiency. Depending on the size of the organisation, up to millions of alerts can be raised every day – the vast majority of them turning to be false positives. Yet, every alert unnecessarily raised requires a decision to be made, logged and possibly audited, translating in huge costs for all players.

b) **Bad end-user experience**. Compliance processes have also substantially undermined the customer experience (both for corporates and retail customers). The millions of false positives indeed translate in a lot of pain for end-users, either under the form of delay in the processing of their transactions or their on-boarding process, and/or under the form of lots of additional background questions routed to them in case of alerts being triggered. In the most extreme cases, this can also result in end-users being prevented access to the financial system: if the compliance cost is potentially higher than the expected revenue from a customer, a financial institution will often simply turn down the customer. From the end-user perspective, today's situation is far from the promised (and expected) frictionless payment and on-boarding experience.

c) **Low effectiveness**. To make it worse, despite all the money spent, the unquestionable commitment of the financial institutions and the frictions created in the customers' experience, the outcome is appalling: The United Nations Office on Drugs and Crime estimated that only 1% of financial crime is prevented.

d) **Slower innovation**. The heavy and inefficient processes are also considerably slowing down innovation in the financial community. A straightforward example is real-time payments. With – depending on the organisations' policies, risk appetite and processes – between 3% and 15% of international payments currently triggering an alert (and therefore requiring some human interventions), the vision for a real-time cross-border payment solution currently seems significantly compromised.

e) **Emerging business threats**. Incumbent financial institutions are increasingly under threat from new players (e.g. fintechs, digital banks). Those new players have understood the end-user frustration and are now aiming at re-designing compliance processes and leveraging new technologies to offer a much better end-user experience. But given the interdependencies in the financial industry, even those new players – while they can fix the processes which are fully under their control – remain dependent on the efficiency of their partner banks' processes.

Clearly the current situation is not sustainable. A radical change has to happen. The good news is that all elements are now there to enable this change.

New technologies can radically improve the screening process

Current processes are still leveraging outdated technologies, typically developed 15 to 20 years ago in the early days of the fight against financial crime. Financial institutions have been relatively complacent about evolving these technologies, essentially because of

a) **Regulatory barriers**. All financial institutions have regular reviews with their regulators to demonstrate the robustness of their compliance processes. These are resource-consuming and stressful exercises for bank executives. And once regulators' comments have been implemented or a path toward implementation has been defined and agreed, there is little willingness to experiment new processes that could risk trigger new regulatory questions. Regulators, although well intended, have unfortunately contributed to a 'if not broken do not fix it' mindset from many bankers.

b) **Lack of innovation from technology providers**. Screening technology providers have had little incentive to innovate. On one side, they were struggling with the challenge of maintaining the several different releases of their software, with most implementations being on-premises installations (and therefore harder to evolve). And on the other side, once regulators had grown relatively comfortable with a solution provided by a software vendor, there was no incentive for that provider to significantly evolve its software and therefore risk jeopardising the market-perceived 'No regulator objection' stamp on their software.

Yet, for those daring to innovate, the reward can be very significant in terms of efficiency, effectiveness and customer experience. A number of new technologies can indeed offer break-through (10x-like) improvements to the screening process:

a) **Cloud computing**. Performance has always been an issue for screening, especially for the time-critical transactions screening process. Algorithms had to make a difficult trade-off in terms of what to screen in priority (typically just the name) and what rules (and in which order) to apply to maximise performance. Efficiency (in terms of false positives rate) was therefore often considered as a lower-priority criterion. The now widely available Cloud Computing technology is revolutionising this, allowing infinite scalability at low cost. New screening engines specifically designed for the Cloud and not hindered any longer by effectiveness-efficiency-performance dilemmas can now deliver considerably better screening results.

b) **Artificial Intelligence**. Artificial intelligence (AI) and regulatory processes have always had a tough time finding a common ground. This is driven by the fact that heavily regulated processes (such as screening) must have a predictable and explainable output, thereby limiting their ability to fully embrace AI. However, targeted usage of AI greatly improves performance. For instance, AI-powered context analysis of the information to be screened (e.g., identification of language/cultural affinity) can allow the selection of the most appropriate screening algorithms, while maintaining predictability and explainability of the result. Likewise, in the post-alert area, operators can benefit from AI-enabled suggestions (based on learned behaviour on similar cases) on whether an alert is likely a false positive – the ultimate decision would however remain human-based.

c) **Geolocation**. Much progress has been made in geolocation that can serve the screening process. If a politically exposed person appearing on a list is known to be living in Paris (France), a smart screening engine will know that a possible match detected on someone living in Versailles (20 km west of Paris, France) is one that deserves attention while a possible match on someone living in Paris (Texas, USA) is most likely a false positive.

d) **Robotics.** In the post-alert resolution, robotics can prove very effective at providing additional context on a possible hit, by enriching the information at hand with relevant insights automatically gathered by robots from other databases, social media, etc. Additional information could be ultimate beneficiary owners, family links, known additional addresses but also images of the person that – when available – could be automatically matched with new face recognition technology. The additional insights will allow the operator to take a faster and often more accurate decision.

e) **Data Cleansing**. Finally, an often under-valued and yet instrumental aspect is the quality and richness of data. That applies to both data that has to be screened (input information) as well as data that input information has to be screened against (e.g., sanctions lists, Politically Exposed People lists). Standardised data (e.g., structured fields for names, addresses and countries as opposed to a string of unstructured characters), richer data (containing e.g. date of birth) and comprehensive end-to-end data (e.g. in a payment, data on the originating party but also on the final beneficiary) can make a huge difference in the performance of the screening process. Today, most cross-border payments unfortunately still carry very little and unstructured information (while richer and structured information is often actually available at the time of the payment origination but failed to be carried through the payment journey). The financial industry is however moving towards using ISO20022 standards for payments with European, UK and US Market Infrastructures announcing implementation dates. Adoption of this structured format should lead to significant efficiency gains.

Those new – yet already proven – technologies are now available and increasingly easy to implement. Embracing these technologies should be a clear priority for every institution. These are low-hanging fruits allowing for dramatic improvements in efficiency, effectiveness and customer experience.

Financial Crime Compliance Utilities are emerging

Beyond the benefits that each institution can get from implementing the latest technologies, significant additional benefits can be unlocked through industry collaboration.

In the KYC area, a success story from SWIFT, the interbank cooperative, can illustrate this point effectively. Five years ago, it created a global KYC Utility for correspondent banking (called the KYC Registry), which aimed at collecting comprehensive and high-quality KYC information on each of the 7,000 banks active in correspondent banking. KYC Information would be directly sourced from each institution (which would only have to submit the information once) and then each institution – through the utility – could then selectively share in a secure way this information with all its counterparties. Instead of having to chase all its counterparties in a bilateral way for the required KYC information, an institution would go to the KYC Registry and request access to all its counterparties - a very efficient process.

Such Utilities can offer multiple advantages to the institutions involved:

a) **Higher efficiency**. Provided that the scope of the Utility is one that allows for de-multiplication of tasks, cost efficiency can be massive. In the above-mentioned KYC Registry, knowing that each correspondent bank has on an average more than 100 correspondents, the cost efficiency gain can be as high as a 100x.

b) **Cost mutualisation**. Beyond the efficiency gains, Utilities benefit from significant cost mutualisation and scale economies allowing institutions to benefit from best-of-breed technology solutions but also access to leading industry resources and skills.

c) **Higher standardisation.** As a necessary condition for Utilities to succeed, institutions need to agree on common processes and practices, which in turn will allow for the emergence of standards (e.g., agreement on which transaction fields to screen against, agreement on the list of documents to request for account opening). This standardisation, as observed in many industries,
subsequently acts as a key enabler for innovation. It is indeed easier for new vendors (or even incumbents) to propose innovative solutions when a standard is being used in the market as it maximises the number of players that can benefit from the innovation (and increases the financial return for the company that has invested to provide this innovation).

d) **Better compliance**. When institutions work together to create a Utility, they rightfully tend to go for a high bar, by sharing best practices and deriving a process and modus operandi, which take the best of the individual institutions' existing processes. Referring to the example of the SWIFT KYC Registry, the baseline of KYC data and documents requested to each institution is higher than what individual institutions would have requested. As the information only has to be submitted once to the Utility, the pain for a specific institution of providing the more demanding information is easily offset by the significant gain of seeing this information leveraged by hundreds of their counterparties.

Not all financial crime compliance utilities attempts have been successful though and unfortunately some institutions had negative experience from failed utilities, for instance in the field of KYC for securities firms or for some domestic retail customers. Yet, successes and failures have now allowed to clearly identify the key success factors for such Utilities:

a) **Mutualise a process that allows for significant synergies and scale economies**. As an example, a regional KYC Utility for international corporates will be more likely to succeed than a KYC Utility for domestic retail clients. Indeed, international corporates have more banking relationships than domestic retail customers, therefore allowing for higher savings through mutualisation.

b) **Think big, start small, scale fast**. Utilities must have a compelling and bold vision to incentivise financial institutions to let go their existing individual processes and embrace a common vision and utility. Yet, too ambitious utilities will face so many issues in their early stages that they will fail to build momentum. Selecting and sticking to a contained scope first, demonstrating success and then scaling up fast is an effective way to ensure success.

c) **Standardise extensively**. Gains from Utilities will only be achieved if the outcome of the Utility work can be integrated easily in the existing processes of the institutions using the Utility. If every single institution still needs to significantly rework the outcome of the Utility to adapt it to its own processes and policies, the benefits of mutualisation will vanish quickly. Standardisation toward the highest level of compliance is the only way forward to succeed.

d) **Set the right expectations – no shift of liabilities**. Even if this would be ideal, there is no hope that financial institutions would be able to shift their liabilities to Utilities. Regulators will continue to hold individual institutions accountable. Yet, that does not prevent financial institutions from leveraging these Utilities by implementing appropriate controls, as they would do for any outsourced process.

In a number of countries, regulators have shown support for such Utilities. This is driven essentially by their desire to improve both the end-customer experience (often heavily impacted by individual banks' sub-optimal processes) and the overall effectiveness of the fight against financial crime. In addition, in Europe for instance, The European Banking Authority (EBA) has published Guidelines on Outsourcing arrangements, which define the rules and expectations for financial institutions to outsource activities to service providers. Such guidelines provide the right context for more Utility services to emerge.

We are still in the early days of Utilities and many more potential use cases can already be identified, like the screening of international payments. A typical international payment involves on average three financial institutions, and often many more. Each of those institutions screens the same transaction against essentially the same sanctions lists. Why would a Utility not rather orchestrate a process that would screen the international payment only once, against the strictest standard shared by the institutions involved in the transaction and dispatch the alerts among those institutions? Efficiency and user experience would improve substantially. Likewise, the painful process – during on-boarding or regular risk assessment of corporate clients – of identifying ultimate beneficiary owners and screening those against sanctions or politically exposed people lists would be another good candidate for mutualisation.

There is momentum in Private-Public data sharing

A final area that can unlock significant additional benefits is data sharing between public entities and the private sector. Recent initiatives, at domestic but also at international level are encouraging (like the Joint Money Laundering Intelligence Taskforce (JMLIT) or the recently announced EU-level criminal law provisions and information exchange).

The scope of private-public partnerships should be as broad as possible and cover over time all areas of financial crime. In the transaction and KYC screening space, there are two high potential opportunities, both related to the lists provided by government agencies:

a) **Quality of sanctions lists**. A tactical (and yet very welcome) improvement would be the issuing of higher-quality sanctions lists and the creation of a feedback loop. Examples of areas that would greatly improve both efficiency and effectiveness of screening would include (1) using a standardised format for an easy automatic downloading and processing of lists, (2) providing richer and higher quality content on each list entry to reduce risk of false positives and – more

pragmatically – (3) ensuring timely release to avoid the week-end rushes. As a positive news, progress is being made with the OFAC leading the way. Importantly a systematic feedback loop should also be implemented so that private entities could easily report operational issues faced on some specific list entries as a way to trigger government agencies to try and enrich those specific list entries.

b) **More relevant lists**. A more fundamental and highly sensitive step would be to progressively expand the content of the lists themselves. There is significant frustration that today's available lists are basically based on yesterday's information, containing only the names of people or entities already flagged by law enforcement agencies (e.g. convicted people, confirmed terrorists). Law enforcements' databases are much richer and also contain very relevant information on suspected people and their relationships. Finding a mechanism and the appropriate controls allowing the sharing of such additional information with financial institutions would have a dramatic positive impact on effectiveness. This will have to be a very careful and iterative journey but with a big potential reward: gone would be the days where we would only stop 1% of financial crime!

It is time to shift gears

Financial crime is a major issue for our community. We must find ways to effectively and efficiently prevent it while preserving the end-user experience. Incremental improvements, iterating on processes and technologies developed more than 15 years ago, will not make it. It is time for the community to shift gears and embrace bolder moves.

The way forward is increasingly clearer and within reach. First, financial institutions, corporates and fintechs should quickly embrace the latest technologies, which can be implemented individually by every player. In addition, at domestic, regional or global level, financial institutions, fintechs and corporates should work together to foster the emergence of more financial crime compliance Utilities, building on the early successes. Finally, public and private entities should work together to allow more data exchanges between the various players.

It is clear from discussions with all the key stakeholders (e.g., compliance officers, regulators, technology providers, banking associations, supra-national bodies) that there is a huge willingness to act and improve the current situation. Technology is now ready to enable it. Let's get started!

Contact Us

info@neterium.io
linkedin.com/company/Neterium
@neterium