LexisNexis®
RISK SOLUTIONS

BRIEFING

The Evolving State of Compliance in Singapore

JANUARY 2017

LexisNexis®
RISK SOLUTIONS

BRIEFING

JANUARY 2017

The Significance of Knowing Your Customer in the Big Data Era

Although small in population, Singapore is one of the most data rich countries in the world, with residents' nine-character personal IDs containing information including their income; career timeline; health status; and travel history. In mid-2015, the Monetary Authority of Singapore (MAS) set up and funded a Fintech and Innovation Group under its Technology Infrastructure Office, to oversee regulatory policies and strategy for technology-based financial infrastructure. The Group has Big Data, as well as cloud computing and the distributed ledger - commonly known as blockchain - under its purview. Big Data and associated technologies are central to the development of the city-state's financial services industry and emphasised by market participants as well as regulators. With the data analytics sector said to add USD1 billion to the Singapore economy by 2017, Know Your Customer (KYC), Know Your Customer's Customer (KYCC) and Anti-Money Laundering prevention efforts (AML) have taken on new significance.

As Singapore works to maintain its position as a preeminent financial centre, expectations around KYC and KYCC compliance continue to escalate. Under the city state's anti-money laundering and counter-terrorist financing rules, banks operating in Singapore must have robust controls to detect illicit funds coming into the financial system. As in many other jurisdictions, this means they are required to identify and know their customers, including beneficial owners of assets held in accounts; conduct regular account reviews; and monitor and report any suspicious transactions. In this context, the first challenge to obtaining the complete KYC snapshot is connecting different sets of information – such as bank accounts and other financial assets held, loans outstanding, and online banking interactions – into one holistic perspective.

> Singapore is ideally positioned to take advantage of Big Data technology for KYC.
> —Chris Foye, LexisNexis

Putting the Benefits of Big Data to Work

For financial institutions, Big Data presents valuable opportunities for improving compliance in the face of regulations that are growing more stringent and recent events, like the 1MDB scandal, that have highlighted the issue of money laundering in the South East Asia market. Many experts feel that Big Data can help streamline essential enhanced due diligence processes by making them more efficient and easier for financial institutions to complete. According to Chris Foye of LexisNexis Risk Solutions, "Singapore

is ideally positioned to take advantage of Big Data technology for KYC given culturally the collection of such data is accepted within the country. As a result, financial institutions are exploring ways they can improve process efficiency through greater collaboration with other institutions and third parties." These sentiments are echoed by Shong Ye Tan, digital business and risk assurance leader at PwC, "Many firms are increasingly relying on Big Data, which involves investment in processes and systems to support it."

The future for Big Data as a valuable compliance tool looks strong but harnessing the benefits of Big Data presents challenges for many financial institutions, including legacy issues, data security, efficiently managing adverse media screening, accountability issues and balancing compliance efforts with core business operations. A financial institution's ability to successfully navigate these challenges will determine how effectively the institution can leverage the value behind Big Data for both compliance and commercial applications.

Overcoming Legacy Issues and Technology Lags

Big Data demands systems that can support it and facilitate seamless information exchange between many different and decentralized departments. Many financial institutions are still working with older systems that are not designed to withstand Big Data demands. Risk aversion, cost impacts and the general tendency for this industry to be late adopters all impact the speed with which newer technologies are implemented and working with legacy systems often reduces the efficacy of a Big Data solution.

According to Shong Ye Tan, "Most organisations we see have infrastructure that has been in place for a while. Given the additional requirements, many of them are assessing whether this infrastructure is meeting their needs, very often via audits." Tan continues "After you put in the rules and keep them for many years it is not certain whether all the monitoring is working the way it is supposed to. Usually you need to improve, and tighten up."

Resistance also stems from players in the financial industry still struggling to fully digest the regulatory overhaul that has followed the 2008 financial crisis and the impacts those regulations have had on many core processes, like customer onboarding. Peter Guy, Editor-in-Chief of Regulation Asia, shares his views, "Not only is this situation a radical departure from the past, but the costs and hence the difficulties are rising. Reforms following the global financial crisis weren't supposed to make banking more arduous for the average person, but it has set back the practice of financial inclusion for a sizeable part of the population in developing countries - migrant workers whose families depend on them regularly being able to send them about USD300 to USD500 a month through money agents."

Information overload ...directly affects business and client relationships.
—Peter Guy, Regulation Asia

Guy continues, “Even eight years after the global financial crisis, institutions continue to struggle with the full implementation of KYC and AML systems. Databases and processes stubbornly remain in isolated silos where the data and managers do not communicate with other parts of the firm. Big Data can also translate into information overload and this directly affects business development and client relationships.”

Guy concludes, “Today’s on-boarding cycle has stretched to as much as 60 days. Bankers worry that automation has not yet made a serious improvement in meeting all the regulatory requirements. Compliance platforms appear to be mired in a constant state of work in progress.”

Successfully Strengthening Security

Another pressing challenge with mining Big Data, as well as other decentralised technology, to inform KYC/KYCC functions, is ensuring the single snapshot can be obtained while maintaining privacy and staying within Singapore’s data protection rules. The fact Singapore is a technically advanced, ‘smart city’ can be a double edged-sword – according to software security group Kaspersky Lab, of all its users attacked by malware in Singapore last year, more than one in 10 were targeted at least once by banking Trojans. Data security issues become a challenge when faced with the complexities of information sharing between different banks and allowing information to be shared across borders.

Authorities acknowledge security is a risk in Singapore. MAS has incorporated it into the Technology Risk Management Guidelines for financial institutions, which requires banks to implement IT controls in order to prevent unauthorised access or disclosure of customer information. At the end of March this year, MAS held a two-day conference at which it explored the use of APIs (application programing interfaces) to allow communication between non-financial apps and banking services. Chief fintech officer Sopnendu Mohanty noted at the time that one robo-advisory service in Singapore already uses APIs for client onboarding.

Data security issues are not a problem within financial institutions, where banks have operational requirements to share data between their different business units, but there are challenges in the areas of information sharing between different banks

and allowing information to be shared across borders. This has led some institutions to consider the possibility of a local KYC utility which would be controlled by members and have the input of the local regulator.

On the first front, Nizam Ismail, partner at RHTLaw Taylor Wessing notes, "Banks have a lot of information they could share. From a macro view it would lead to a more efficient process for client due diligence, but they do not do that at the moment, which could be due to confidentiality or secrecy issues. One solution would be to develop a closed community which would enable restricted access to data. This might be the only way to freely share KYC information to reduce duplicative processes while adhering to privacy protection rules," he believes, "There are innovative ways in which you could share information within a limited circle of people without overly compromising issues of confidentiality and privacy."

Chris Foye continues, "This concept of a closed community with strict access controls designed and maintained just for participating members would also allow members to control and dictate the process and standards followed. It should not be restricted to the on-boarding of corporates, but be extended to individuals to ensure the real benefit in terms of efficiency, improving the customer experience, identification of networks for the purposes of detecting illicit money flows etc. are realised."

If this is to happen, it will be important for organisations to take care when they transfer information out, in particular to make sure that those institutions they share information with have a similar level of controls.

In terms of cross-border transfer of information, Eric Chan, financial services regulation partner at Singapore law firm Shooklin & Bok, sees the main challenges are jurisdictional, "Singapore does not have any specific requirement that financial institutions keep their data centres and data onshore, but several other countries in South East Asia do. Individual jurisdictions have different rules so from a Pan-Asian perspective things are not going to be that straightforward. But, in Singapore, banking secrecy should not be a problem as there is stringent control of use of subcontractors and service providers who have to commit to give MAS access, even if it is not the regulator of the [cross-border] client," he says. Institutions that use service providers face another problem, according to Chan: "The tech companies have certain exposures to other jurisdictions in the region with different rules, so the issue can get very complicated, particularly if they have multiple tenants."

Capturing the Advantage of Adverse Media Insights

Adverse media screening is another way in which Big Data can be a boon for the efficiency and compliance of financial institutions in Singapore when conducting KYC and KYCC. Effectively managing adverse media data to quickly

garner valuable decisioning information without having workflows impacted by the drag of false positives remains a challenge for many financial institutions to overcome.

The practice of screening media to find clients or politically exposed persons, who may be involved in risky areas such as tax evasion or fraud or that can link them to wider family networks that might conduct transactions on their behalf, is becoming increasingly automated. This is particularly true among large institutions with vast numbers of clients across multiple business lines, who use Big Data to normalise, link and structure the information they have on clients. Some systems can include real time alerts, allowing a bank to take immediate action to reduce exposure to a risky account or individual and share information across multiple business lines - given Singapore's supportive regulation in this area.

It remains an imperfect science, as by its very nature adverse media screening can only look at information already available in the public domain. It cannot look at criminal records in Singapore let alone other jurisdictions which bring money into Singapore, for example, given the abovementioned cross-border data concerns in other areas of KYC/KYCC. For the foreseeable future, the human element remains vital in the adverse media screening process, as well as other areas of Big Data. According to the Infocomm Development Authority, the number of data analysts working in Singapore will need to increase by a third over the coming three years in order to meet demand.

This is particularly true given the incidence of 'false positives', where systems flag up incidences of sharp practices which eventually prove to be false. Shooklin & Bok's Eric Chan observes, "There have been problems where screening systems threw up hundreds if not thousands of false positives. This ends up with institutions having to hire a team of individuals to eyeball the hits and screen out those false flags." Chan continues, "It is better now, as screening systems have become more intelligent and are able to throw up more meaningful hits. But you still need a human element. Most banks have dedicated compliance personnel whose sole function is to review hits."

False positive reduction is key for any screening system along with choosing a provider with a comprehensive approach to monitoring adverse media.

—Chris Foye, LexisNexis

Chris Foye adds to this point, “False positive reduction is key for any screening system along with choosing a provider with a comprehensive approach to monitoring adverse media. The main challenge with adverse media is it is unstructured data which requires substantial compliance analyst review. A provider that monitors the media whilst providing a structured profile which can be leveraged efficiently by a screening platform can significantly ameliorate the false positive rate.”

Managing the Pressing Risk of Personal Accountability

The importance of a viable combination of stringent KYC and KYCC processes and a thorough AML prevention protocol is illustrated in the levels of accountability meted out when issues tied to non-compliance arise. In Singapore, cases of market abuse can lead to banks being held liable in cases where they have not had strong compliance programmes. Under the UK’s Presumption of Responsibility, senior managers can be found guilty of misconduct merely by virtue of their responsibility for an activity in which rules have been broken. This human element requires strong leadership from senior management in ensuring adverse media screening and other KYC/KYCC measures are effective. Indeed, some jurisdictions have already incorporated this into regulation.

RHT Law’s Nizam Ismail provides his view of the current situation in Singapore, “For other cases such as regulatory and money laundering breaches, there have not been any prosecutions against banks or financial institutions, let alone against individuals,” he notes, “We are a couple of steps away from that in Singapore, and when it comes it will have quite a few controversies and implications. In other parts of the world, heads of compliance need to personally sign off on AML processes to confirm they are sufficient, but again there is no similar requirements for most of South East Asian jurisdictions.”

For now, financial institutions in Singapore, and other jurisdictions in Asia Pacific with a similar lack of specific regulations on management responsibility, will need to ensure the lead comes from the top. “If you look at all the big fines that have been handed to large financial institutions elsewhere this is not something you can pay lip service to,” offers PwC’s Shong Ye Tan, “It will be important to get competent people with the right skillsets to run departments such as KYC and to get independent reviews of some of the processes because they should be aware regulators are concerned and will check.”

Chris Foye of LexisNexis concludes, “Such reviews must extend to the screening systems and data in place and the current rules and configurations to ensure they are up to date given changing regulation and the risk landscape.”

Balancing compliance with commerce and innovation

As an increasingly important destination for cross-border payments, Singapore must strike the right tone in dealing with the risks and balancing compliance demands with commerce opportunities. Cross-border electronic payments and mobile remittance are a particular area of concern in Singapore, given its status as a way station for much of the financial flow across Asia Pacific. According to a 2014 survey by PayPal, Singapore's online commerce market grew 38 percent a year from 2011 to nearly USD3 billion in 2014, and is expected to reach USD4.92 billion by 2018. And, according to technology and market research company Forrester, 60 percent of online sales in Singapore result from cross-border transactions.

Against this backdrop, managing and understanding data is a particularly pressing issue in dealing with mainland China, Malaysia and Indonesia, where institutions increasingly need not just KYC but also KYCC. Singapore, and international authorities, have been proactive in dealing with the issue. The earliest measures to touch on the issue are contained in 2007's Computer Misuse and Cybersecurity Act. This was followed by the government establishing Singapore's Cybercrime Command, and then in April 2015, Interpol set up a cybercrime centre in the city state.

In recent years, Singapore's growing status as a fintech hub has made maintaining this reputation for robustness a balancing act between commerce and compliance. DBS CEO Piyush Gupta said recently the bulk of its expenditure goes toward middle and back-end functions. For now, market commentators believe Singapore is taking the right approach. "There is a sandbox framework that allows payment companies to simplify KYC processes for transfers below a certain amount," offers PwC's Tan. "They can also talk to MAS about regulatory challenges. Proof of concept allows a good idea to be experimented with rather than killed because of some possible non-compliance with regulation."

As part of this simplification of KYC processes, fintech companies are actively adopting identity verification, document authentication and AML screening technologies that can provide a seamless end user experience, reduce customer abandonment rates whilst still mitigating AML and fraud risk.

BRIEFING

LexisNexis Risk Solutions can help your business harness the benefits Big Data can bring to your core operations while strengthening key compliance initiatives. We combine the industry's most robust data reach and substantial global sanctions coverage with powerful analytics and proven technology solutions that quickly connect your business to an optimized viewpoint of a consumer or business. Many of our solutions run on the backbone of our powerful HPCC Systems® which enable us to significantly accelerate the processing of large volumes of data from a myriad of public and proprietary sources. We deliver a faster analysis across distinct data sets and provide stronger linking of critical data points. This can help your business quickly eliminate data redundancies, enrich your existing data with actionable insights and improve the overall efficacy and value of your customer data.

At LexisNexis, our solutions are designed to help your business access a synthesized picture of your customer and the risk they may, or may not, pose to facilitate faster, more well-informed decisions across the entire customer lifecycle. We can help your business truly know your customer and understand the intricacies of their critical relationships and connections. Our solutions highlight and help identify potential AML risk before it impacts your business. By leveraging tools from LexisNexis you can implement a comprehensive compliance workflow without interrupting your core business.

Contact us to see how we can help you balance the goals of protecting your business and maintaining profitable operations.

For more information
Visit www.lexisnexis.com/risk/apac
Toll Free Singapore: 800.120.6351

LexisNexis®
RISK SOLUTIONS

About LexisNexis Risk Solutions

LexisNexis Risk Solutions is a leader in providing essential information that helps customers across industries and government predict, assess and manage risk. Combining cutting-edge technology, unique data and advanced analytics, LexisNexis Risk Solutions provides products and services that address evolving client needs in the risk sector while upholding the highest standards of security and privacy. LexisNexis Risk Solutions is part of RELX Group plc, a world-leading provider of information solutions for professional customers across industries.