

# 2017 Asia Pacific Vendor Landscape: AML Solutions

A look at the key providers of  
anti-money laundering solutions in Asia  
A report by Kapronasia

Evaluation

# Table of Contents

Introduction.....	3
AML Industry Trends.....	5
Industry Lessons.....	9
Vendor Analysis - Key Findings.....	11
Asia Pacific Regional Requirements.....	15
Industry Requirements Based on Size.....	17
Comparing Leading Providers.....	22
ACI Proactive Risk Manager (PRM) for AML.....	24
BAE Systems NetReveal.....	28
FICO Siron.....	33
Fiserv.....	38
Intellect Design Arena AML.....	41
LexisNexis Bridger Insight XG.....	47
NICE Actimize.....	50
Oracle Financial Services Anti-Money Laundering.....	56
TCS BaNCS.....	62
Temenos.....	68
Kapronasia Competitive Index: AML Solutions.....	72
Conclusion.....	73

## Methodology

This is Kapronasia's first report profiling anti-money laundering (AML) solutions in Asia as well as the trends that are driving their adoption. To analyse the capabilities of the AML solutions in the marketplace, Kapronasia invited nearly 30 firms to participate in the AML study. Firms were asked to provide written descriptions of their AML solutions as well as solution details around particular measurement points. In addition, Kapronasia asked for client-level details about current deployments in the Asia region. Of the 30 vendors contacted, just under half had AML solution offerings for Asia and, of those, 10 agreed to participate in the study.

We are seeing a rise in the globalization and liberalization of financial services across the world today. With this development comes a rise in financial crime. Anti-Money Laundering (AML) technology is becoming an essential tool in the overall strategy to fight financial crime. This is particularly prevalent in the fast-growing Asia-Pacific region, where economies are developing rapidly. Cybercrime, especially crime related to terrorism, has forced governments to focus on financial transaction processes in order to ensure the safety and legitimacy of the financial services industry.

Globally, cooperation with national regulators has been at the forefront of the industry. In several instances, the leading jurisdictions have been implementing new regulations that originate from this global cooperation. The regulatory standards have given uniformity of approach, which is desirable from a technological point of view, thus allowing for easier interaction and collaboration in the development and implementation of AML systems.

The rise in advanced machine learning capabilities is also playing an important role in the growth of AML systems. While the industry continues to be people intensive, we are seeing a move towards more skill- and expertise-based roles for employees, with repetitive or low-level tasks being performed by the AML platforms.

Further, allowing financial services firms to handle growing transaction volumes has the potential to improve AML capabilities. Without the improving technology, these firms would struggle to meet their requirements in a cost-efficient way. Large banks employ hundreds, if not thousands of professionals to manage their AML requirements and fight financial crime. This figure would be much higher were it not for machine learning and greater commoditization of the underlying technology. This is particularly true with regard to employing cloud services, and the utility models used to perform underlying KYC and AML processes common within the industry.


Asia is a very diverse region, with multiple jurisdictions and financial markets that have varying levels of maturity. AML regulations and requirements often differ across countries, and Asia-Pacific is a more complex market to address compared to Europe or North America. We have also seen the AML industry in Asia change over time. In the past, most of the countries in the region were content to meet the regulatory requirements of the leading global markets such as the US. However, in the last decade, we have seen a regulatory impetus to ensure that the AML platforms meet the specific local and national requirements across the various jurisdictions.

Singapore – a major financial hub – has been at the forefront of this development along with other jurisdictions, such as Hong Kong, Japan, and Australia. Several participants in this study have also commented on the increasing sophistication of AML requirements in large economies such as China and India. Amidst rapid economic growth and a rise in cybercrime threats, these economies are trying to ensure that they have the right frameworks in place with regard to financial crime, and specifically AML.

**Anshuman  
Jaswal**

**Director**

**kapron  
ASIA**



Several participants in this study have also commented on the increasing sophistication of AML requirements in large economies such as China and India, which are trying to ensure that they have the right frameworks in place with regard to financial crime and specifically AML amidst rapid economic growth and rise in security threats including cybercrime. Systems also are moving to be more 'holistic' in order to allow firms to deal with all these areas of concern through one platform, as much as possible.

Several countries are putting their own regulations in place in line with the global Financial Action Task Force (FATF) guidelines. The Asian members of the FATF include Australia, China, Hong Kong, India, Japan, South Korea, Malaysia, Singapore, New Zealand and the Gulf Co-operation Council (GCC). While countries such as the US have played a leading role in dealing with money laundering in the past, having a body such as FATF is a very efficient way of dealing with the issue, allowing jurisdictions to learn from each other while putting in place measures that are coordinated, synchronized, and streamlined. This takes into account the fact that most money laundering occurs across national boundaries, and often targets the jurisdictions that have the weakest AML laws.

This report looks at the AML systems being employed in the Asia-Pacific region. It begins with an overview of the important recent trends in the industry, the lessons to be learnt from recent AML related events worldwide, a comparison of the leading AML solutions across certain parameters, and the change drivers for the AML industry across Asia. This is followed by a discussion of the leading product offerings in the AML space and a comparison of their features and important functionality.

We hope you enjoy reading this report as much as we did writing it.

# AML Industry Trends

With global markets developing rapidly, there has been significant change in the AML industry. Although many of the trends are unique to specific jurisdictions, there are some overall industry trends taking shape.

**Digitization** is an important trend in the financial industry. Financial services providers are moving towards digital and mobile channels, and virtual currencies are also becoming more common, which is changing the AML focus of the industry. AML systems are also adapting accordingly to ensure that the large volumes of digital transactions meet with the same levels of scrutiny,

**Beneficial ownership** is becoming an important focus area for regulators and firms. Some examples of recent regulations globally include the Fourth Money Laundering Directive, FinCEN, and MAS 6262. The recent rules require financial services firms to identify the “real” people behind corporate accounts. This creates challenges for organizations as it increases the length and complexity of the onboarding process. It also brings an additional operational burden of managing corporate accounts and keeping the ownership information current. In some Asian jurisdictions, financial service providers struggle with validating ownership information because there are no national level ownership repositories available. In other jurisdictions, more progress has been made and public ownership databases are becoming available.

Throughout the Asia-Pacific region, there is a high level of international trade and economic dependence on trade. As a result, **trade based money laundering is also an important concern for regulators** who are striving to ensure that terror, drug related, and human trafficking related laundering does not happen.

**New risk based methodologies are being utilized by regulators and financial organizations.** Model risk management is an important tool that allows firms to handle the growing complexity that AML systems should deal with. An important step in this regard was the guidance provided by the OCC in 2011 requiring that financial institutions verify that models were performing as expected in accordance the designated objectives. Some Asian regulators have built additional regulations on top of those, including the Hong Kong Monetary Authority (HKMA), the Australian Transaction Reports and Analysis Centre (AUSTRAC), and the Monetary Authority of Singapore (MAS). This means that firms have to develop a deeper understanding of their AML systems, their analytical capabilities and how they work. It also puts an additional operational burden on the compliance functions and increases the cost of compliance.

**AML systems are using the some of the latest technology including advanced machine learning, artificial intelligence and natural language processing.** In addition to making existing processes faster, it also allows the larger financial firms to deal with rapidly growing transaction volumes. Similarly, other constraints that the financial institutions have include regulatory inspection and increasing cost pressures. Artificial intelligence-enabled solutions are expected to reduce these challenges, reduce costs, and increase efficiency. While AI can come up with predictive scenarios and machine learning helps considerably in managing false positives and false negatives. Predictive

analytics provide an objective view of data related to risk along with mitigation plans. It provides a fair idea on the feasible thresholds for configuring various money laundering patterns.

The rapid technological strides and cost pressures in the last few years are leading to the convergence of compliance functions across the firm. In the next few years, **we will see the convergence of various risk and financial crimes compliance across AML, Fraud, combating the financing of terrorism (CFT), Foreign Account Tax Compliance Act (FATCA) compliance, and anti-bribery regulations.** These areas have similarities across frameworks/constructs, technologies and processes used as a part of a bank's risk management. There is demand now to integrate these solutions and implement a unified solution at an enterprise level, spanning across all the lines of business. This would help provide holistic view of the risks and threats posed.

Financial organizations are faced with ever increasingly stringent deadlines to meet regulatory expectations. They are looking to reduce the manual effort and to substantively automate the regulatory and compliance processes to meet shrinking time-lines. There is **a continuous effort in AML, like other compliance functions, to automate the repetitive processes to reduce compliance costs** and focus human effort on more pressing concerns such as alert and case management. Robotic process automation (RPA) is an essential tool in this endeavor. In RPA, a bot performs the same tasks as a person and is basically the application of technology to mimic the actions of a human. It captures all process related details and stores them for auditing purposes. The trend is to use RPA in KYC information gathering and validation, real time payments screening and automated management of false positives to address the pain areas of AML compliance.

Besides performing risk assessment of customers, **banks and other financial organizations also need to ensure the conduct of their employees is above board.** AML systems are using behavioral analytics for this purpose. This enhanced surveillance includes trade and communication data. Several global regulators, including Asian regulators such as the MAS and the ASIC have recommended preventive measures covering employee conduct and governance of the firms. To determine normal and baseline behavior, firms utilize a wide range of data that include communications, transactions, and HR data. Using that, firms can determine deviations from individual's normal behavior and can use that to calculate a risk score for the individual, enabling the firm to analyze whether the individual could be putting the firm at risk.

**Financial inclusion and financial transparency is an increasingly important topic for the region,** and globally, with countries like China adopting innovative and systematic means to assess an individual's creditworthiness. In India, the removal of large denomination notes and the sudden shift from a cash-based society is encouraging people to open accounts and to access the financial system.

**An emerging issue related to financial inclusion is de-risking.** It refers to instances in which financial organizations are closing accounts based on a few critical customer factors, such as geography or business type, thereby reducing their exposure. Since it goes against the prevailing ethos of increasing financial inclusion, the trend has recently been criticized by regulatory bodies and raises concerns about financial inclusion and movement of risk to other, less transparent parts of the financial system.


As mentioned earlier, cost pressures and tight time-lines are ever present constraints for financial institutions today. As a result, **many institutions are looking at how they can drive efficiencies in their KYC/AML process.** Firms that are able to achieve greater efficiency can derive a competitive advantage. On an industry level, the drive to improve efficiency has led financial institutions to consider the advantages of a utility model for KYC. In such a case, documentation is pooled, processes are centralized and a degree of standardization can be applied. At a regulatory level, countries such as Singapore and India have made some headway in this regard. Some banks are also working together to discuss the best approach and the advantage of a global utility versus a local / regional utility that will be more tailored to their requirements.

**Firms using AML systems are managing events and alerts more effectively.** In the past, some financial institutions have struggled to manage the alerts that are generated by their rules based detection systems. Many of these alerts are false positives or of very low value to the investigators. While these systems are good at proving to the regulators that the financial institutions are compliant with the regulations, they generate a lot of noise. This is an important area of focus for financial firms today.

The quality of data used for AML systems has always been an issue that needs to be addressed, and this is expected to continue in the future as well. But regulators such as the New York DFS are now **beginning to focus on the firms undertaking validation of the integrity, accuracy and quality of data** to ensure that accurate and complete data flows. In addition to data accuracy, the mechanisms to transfer data are also under focus, with the intention being that there should be no reduction in data integrity due to inadequate monitoring or filtering systems.

The recent rise of FinTech has meant that there are new opportunities for AML vendors, and new industry segments to monitor for the regulators. Even outside AML, regulators have recognized the FinTech trend and encouraged firms in the space. **In FinTech, and some other markets such as gaming and gambling, there is a need to establish compliance processes from scratch,** which is where Financial Crime vendors can be of great help. While obtaining data in the gaming industry for AML purposes might not be straight forward, there is a need to take a similar risk based approach to AML. The techniques used are expected to remain the same, although the requirements are different.





In addition to the new breed of FinTech firms, **regulators are also moving from monitoring banks, to other existing financial institutions** that can be a source of systemic risk, such as insurance and securities, money transfer / remittance companies, and peer-to-peer providers.

With a rise in the levels of terrorism globally, there are **aggressive efforts to tackle terrorist financing**. Several Asian regulators have indicated that terrorist financing is a high priority issue. However, finding terrorist financing activities can be challenging as they often involve smaller cash amounts that sometimes go undetected by current thresholds set on AML systems. Therefore, organizations need to fine tune their AML controls to identify these activities.

The financial markets globally have been rocked by several scandals, including the Asia-Pacific region. This has put the spotlight on various regulatory regimes and prompted regulators to act quickly to protect the integrity of the financial system. As part of this effort, there is a **greater focus on personal and civil liability** within the financial services industry. Financial executives are being held responsible and liable for anti-money laundering compliance, and the liability is not compartmentalized to the overall department or function alone.

The Asian AML industry has been quite labour intensive in the past. It is estimated that labour costs account for nearly four-fifths of Asian AML compliance spending. Hence, **technology use at AML operations in Asia is considered somewhat immature**. But Asian banks and other financial service providers are now trying to change this by using more modern AML systems and automating compliance processes where possible. Hence, in the future, we expect AML functions in Asian firms to resemble their US and European counterparts more closely.



# Industry Lessons

Although regulators' AML expectations are consistently increasing, there have not been any material changes in the foundation of money laundering regulation for over 20 years. Yet, organizations are still being fined for money laundering related issues, as gaps continue to exist even within the most robust AML programs.


In addition, fighting financial crime and staying compliant is an ongoing process. Businesses tend to be in different maturity stages regarding implementation of the tools that they need to protect themselves. A comprehensive AML program starts with a documented risk policy, detailing the organizations risk appetite and risk based approach. Lack of protection can lead to failure of programs, as well as failure in executing adequate procedures to implement money laundering policies, not to mention potential financial loss. This has resulted in financial services organizations realizing the importance of AML compliance and gained the commitment of senior management.

Banks generally only have a view of their own customers, accounts, and transactions. When money launderers make use of multiple banks to undertake 'layering' to hide the source of their funds, individual banks may not be able to detect this. If this is the case, the regulators must take responsibility, as they have a better overview of activities that occur across banks. Basic rule-based systems have difficulty dealing with the mass of data that is being created, and will frequently generate high false positives, or miss actual alerts.

However, AML systems need to be equipped with better detection functionalities, such as risk-based analysis or other forms of advanced analytics. Regulations are constantly evolving and as new information becomes known about these types of reports, it is highly anticipated that the regulators will continue to scrutinize banks further. For example, the Ultimate Beneficial Owner (UBO) rules that have come as a direct impact of the Panama Papers.

After a risk policy is set, processes and procedures can be designed, ensuring the risk policy is being implemented. Technology plays a major role in this process since it can be used to automate many of the processes involved, thereby increasing the overall program quality and consistency, but organizations should also be aware of how it is being used and be certain that it addresses the specific risks for their own organizations. For example, when detecting suspicious activities, models need to be based on the organization's services and products to ensure relevant data is captured and analyzed effectively.

Firms should ideally have automated mechanisms to configure the thresholds rather than to configure the thresholds manually. When customers abandon automated processes and depend on lengthy manual processes, they are put at a disadvantage, miss opportunities and become exposed to potential reputational damage. It is crucial to identify the ultimate beneficiary of the accounts held in the firms and that needs to be included in the KYC process. In most instances, prosecution in money laundering cases is stuck because financial institutions are unable to provide the ultimate beneficiary information.



There is a growing need for information sharing among industry participants for fighting financial crime and money laundering. If financial institutions start to share information, they will be able to identify more cases of money laundering. Centralizing into one enterprise-level KYC database (if not at country level) helps with centralized KYC checks.

Countries, like India, have already started the process of centralizing KYC at country level, where a database will have the KYC details of all clients. This database can be tapped by Banks across the country to access information on Customer Due Diligence & Enhanced Due Diligence. Suspicious transactions require substantial enhanced due diligence. Additionally, employee fraud needs to be checked by the firms and banks, as most money laundering cases have showed that there is insider collusion.

While it is difficult to predict data breaches and information leaks, it is anticipated that regulators are pushing for further convergence of fraud and AML, along with the addition of cyber-related events in future reporting and operations. Recently, we saw a case in which money launderers used shell corporations to shield their true identities and use the corporations and corporate accounting and finance systems to launder the money. The Panama Papers (Mossack Fonseca) is an excellent example, highlighting the limitations and gaps in financial institutions' approach to gathering beneficial ownership information (increased emphasis on knowing your customers' customers, or KYCC).

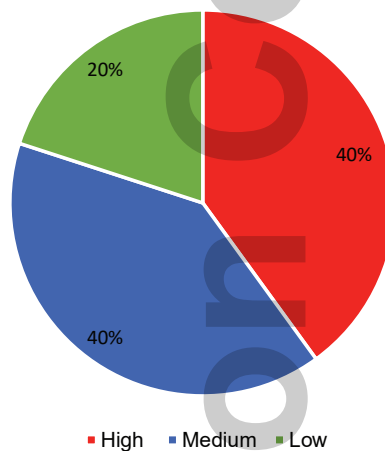
Another area of concern is on the use of trade finance to launder money. Regulation in this area is still evolving. As regulators and financial firms get more adept at protecting the core retail financial system from broad based abuse from money launderers, drug traffickers, and tax evaders, these bad actors are expected to move to other areas in financial services such as mortgage financing, corporate accounting systems, and trade finance.

# Vendor Analysis - Key Findings

As part of the vendor survey, we covered a number of different data points which are summarized at a high-level below.

Figure 1 depicts the number of users per solution across the various vendor offerings. Four vendors have a 'high' number of deployments in Asia (more than 40), while another 4 have 'medium' (between 20 and 40), while 2 vendors have 'low' deployments (less than 20).

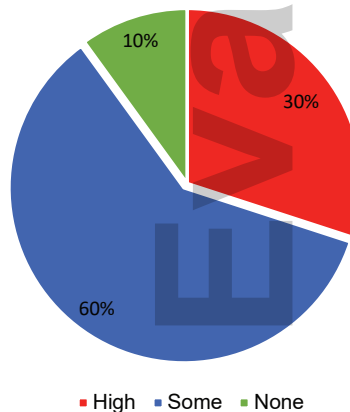
**Figure 1 - Number Of Users Per Solution**



Source: Kapronasia

Figure 2 shows whether the various vendors believe that there are significant differences in AML requirements between APAC and other regions globally. Three vendors believe there are highly significant differences, six believe there are some differences and one stated that there are no differences in the regional requirements.

**Figure 2 - Difference In AML Requirements Between APAC And Other Regions**

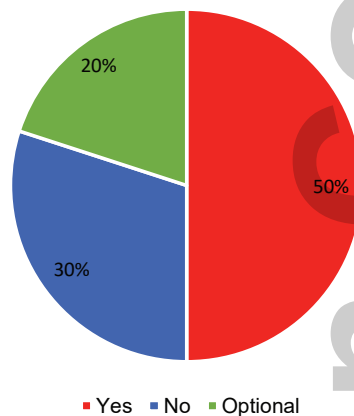


Source: Kapronasia

Figure 3 illustrates the availability of on-boarding functionality across the various solutions. Five solutions provide on-boarding functionality as part of the product, three vendors do not provide such functionality, while another two provide it as an optional module.

---

**Figure 3 - Availability Of Onboarding Functionality**



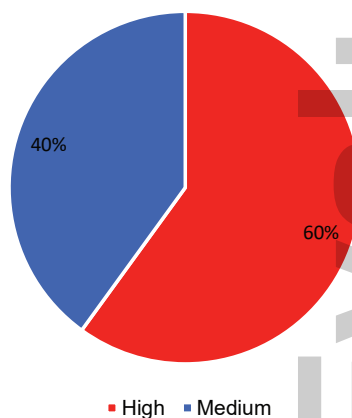
---

*Source: Kapronasia*

Figure 4 below looks at the level of advanced analytics available to users of the various AML products in Asia-Pacific. Six of the vendors provide advanced analytics as part of the product, while another four provide some analytics but it is not necessarily advanced.

---

**Figure 4 - Availability Of Advanced Analytics**



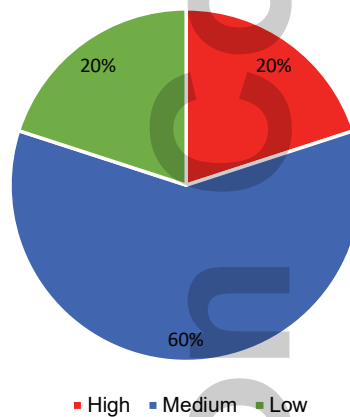
---

*Source: Kapronasia*

Figure 5 shows the level of machine learning and artificial intelligence capabilities that are provided by the vendors. Only two of the vendors provide advanced machine learning capabilities. Six provide some machine learning capabilities, while another two provide a low level of machine learning technology in their respective products.

---

**Figure 5 - Level Of Machine Learning And AI Capabilities**



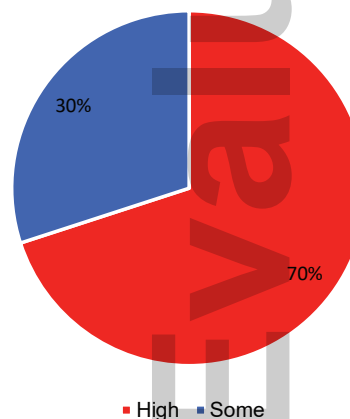
---

*Source: Kapronasia*

Figure 6 depicts the level of pricing flexibility of each of the vendors we spoke to. Although of course a lot of this will come down to the actual discussions, seven of the vendors indicated that they had a high level of flexibility, while 3 indicated that they had some.

---

**Figure 6 - Flexibility In Pricing On Part Of Vendor**



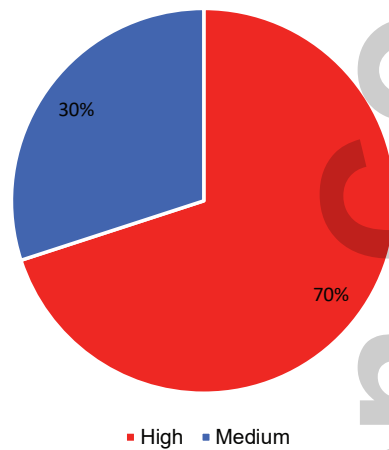
---

*Source: Kapronasia*

Figure 7 looks at the openness of product architecture from a technology perspective. Seven of the vendors indicated that their solution had solutions have a high level of openness from an architecture viewpoint, while the remaining had some openness.

---

**Figure 7 - Openness Of Architecture**



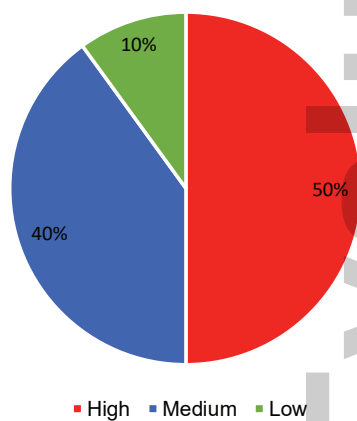
---

*Source: Kapronasia*

Finally, figure 8 illustrates the scope for customization of the solutions by the respective users. Five of the products allow a high level of customization, while three allow for some customization, with one vendor allowing for very little customization.

---

**Figure 8 - Scope For Customization Of Product By User**



---

*Source: Kapronasia*

# Asia Pacific Regional Requirements

AML requirements across various geographies differ, and, among other factors, depend on financial market maturity and integration with the global financial system. The Asian market has a wide spectrum with regard to AML regulation development. High regulation regions include Singapore and Hong Kong, developing areas include China and South Korea, and areas with no AML regulation include North Korea and Iran.

The level of sophistication of compliance practice, and AML regulatory requirements, varies significantly among countries. Certain countries, such as Singapore, Hong Kong, Australia, have very stringent regulations, while other countries are in the process of enhancing their AML framework. To understand the uniqueness of each country, one must have a dynamic mindset, as the markets are so diverse, unlike the market similarity in Europe and North America.

For some countries, the banks are more local in their outlook, and do not serve international markets. In such a case, it is usually adequate for the local banks and financial services providers to meet their domestic regulatory obligations. In the leading financial centers such as Tokyo, Singapore and Hong Kong, the AML regulations and compliance is more global in nature and local firms' policies compare favorably with their European and North American counterparts. From a regulatory point of view, there is a higher level of overlap across the various jurisdictions in the Asia-Pacific because the regulators work closely with each other and often make rules to deal with similar risks and challenges.

For the APAC region, it is important to note that there is also an overlap in regulation from a regional and global perspective. The regional and global companies operating in geography have to take into account local, European and American regulations. If they are dealing in multiple currencies, then compliance procedures have to consider international regulations. The firms in the region are primarily following the Financial Action Task Force (FATF) standards, with several jurisdictions including such as in Japan, South Korea, China and Australia endeavoring to upgrade national regulation to FATF levels.

Financial service providers in FATF member countries (including China, Japan, South Korea, Malaysia, India, Australia, and New Zealand), must comply with FATF recommendations.

As FATF is the leading body for issuing AML norms globally, the mandatory requirements in AML market are standardized to a high degree. In addition to the FATF guidelines, APAC has regional groups that have been created to curb money laundering activities. The Asia Pacific Group on Money Laundering (APG) is one which includes all countries in the Asia-Pacific – 41 members – as well as some international and regional observers. These members collaborate and have put in place coordination mechanisms to efficiently combine resources to combat money laundering and terrorist financing.

The APAC regulations are relatively similar to other leading regions in the world, differing only in their focus points. Remittances, money service business transactions, and trade based monitoring seems to be the main focus in the



region. Further, the rise in scrutiny over trade finance has been a primary topic recently in the region leading to new methods in screening both letters of credit (LOC) and bills of lading. Additionally, the transaction volumes like accounts, customers, and transactions in Asia are generally larger than in other regions, especially in countries such as India, China, and Indonesia. As a result, compliance functions in firms in Asia-Pacific are more decentralized and compliance professionals at the branch level are more empowered to make critical decisions, as compared with a more centralized approach in North America and Europe.

In terms of the overall approach, the Asia-Pacific region follows much of the same compliance philosophies as in North America and Europe. However, there are some subtle but critical nuances with these markets. For example, less scrutiny exists with regards to customer due diligence (CDD) in some markets in the APAC region, and sanctions seem to be viewed differently in some markets. Firms that commit wrongdoing in the APAC region are generally penalized less than those in other regions (North America, Europe) in terms of the frequency of their fines and the magnitude. Thus, with North America and Europe raising billions of dollars through fines, it is obvious that there is less AML urgency in Asia.

Some of the region specific regulatory development includes:

- In Singapore and Australia, there is a growing interest in monitoring Trade Finance Based Money Laundering (TBML). Australia is monitoring all transactions made by foreign individuals.
- In China, there is a focus on identifying and matching Chinese Commercial Codes in transaction screening.
- Recent digitization of currency initiative in India has significantly impacted the KYC and on boarding systems during the transition phase. This is also producing a lot of activity in the AML transaction monitoring area with an anticipated increase in transaction volumes.
- The South Korean regulator has issued new regulations governing data privacy, encryption and security requirements which are unique to that country. South Korea is working to enhance their AML regulation in preparation for the next FATF mutual evaluation.
- The Thai government has recently launched an e-payment system. Across Asia, the increased usage of e-wallets means that individuals may carry multiple IDs and therefore anti-money laundering systems need to enhance their ability to aggregate data across multiple devices.

# Industry Requirements Based on Size


## General AML requirements

From a regulatory perspective, there is no difference in AML requirements for small and large size organizations and are all expected to address regulatory requirements regardless of size. AML requirements of any financial institution is governed by the regulatory needs of the Financial Intelligence Unit (FIU). Regardless of the size, firms are required to perform KYC/CDD for customers, perform ongoing monitoring of transactions, file STRs, etc. The main difference seems to be that the thresholds configured for monitoring are more dependent on the size and the type of business of the financial institution. The difference is also in the methodology in which watch-list scanning is used. Large firms, due to the volume of payments and related processing, have online integration for watch-list scanning. On the other hand, small firms use watch-list scanning only as an end of day process. In addition, there are differences for firms in different industries, such as banks, insurance, securities, remittance companies, etc., where the operations and monitoring scenarios can be different.

While the requirements do not really differ for firms of different sizes, the resources being deployed do differ across the Asia-Pacific region. There is a shift in risk, and smaller institutions are increasingly at higher risk because usually do not have a separate function focused on financial crime compliance, and so at smaller institutions the compliance personnel often work across different functions. By comparison, larger institutions tend to have specialized professionals focusing on specific compliance functions. This information is widely known, with the result that smaller firms are often the target of money laundering and criminal activity, to exploit their relative weakness. To this extent, a case can be made for regulators to ensure that enterprise-grade compliance capabilities is made available by every type of player in the financial services space, including e-commerce companies, FinTech firms as well as banks.

At large firms the major concerns are risk mitigation, reputation damage protection and financial implications of crimes and fines, whereas for small firms the major concerns are risk mitigation, transparency and regulatory scrutiny. The larger firms generally require the AML solution to be interfaced with many different systems and have an emerging need for handling large volumes of unstructured data. They also require more real-time online reporting and transaction monitoring unlike small sized firms. Since large firms generally have a global presence, they require composite reporting for every region. These firms will have multiple lines of business (LoBs), and this means that the AML solution ideally needs to be an enterprise level solution catering to multi entity data handling and reporting.

From a resource point of view, larger financial institutions have bigger budgets to support a great number of staff that can work in specialized groups. As such, larger institutions appear to require more configuration and customization to the products than smaller firms which typically have less staff and budget to be able to support such changes to the solution.



From a monitoring perspective, there is not much of a difference between large and small firms. However, the architecture and complexity of their solutions can vary based on the number of resources, business processes, etc.. For example, a small firm running a limited number of products with small transaction volumes may select a small set of scenarios, utilize standard out-of-the-box work-flows and have simple organizational structure and assignment strategies. Large firms with a global footprint require sophisticated hub installations, processing batches from multiple countries, with a large compliance workforce requiring more bank specific work-flows, organizational structure and assignment strategies.

## **Use of unstructured data**

Reputational risk is one of biggest drivers for AML initiatives within an institution, and using unstructured data can help reduce such risk. However, unlike structured data, which, when combined with advanced-matching technology can significantly reduce false positives, unstructured data still poses a challenge in managing the number of alerts and the potential level of noise.

As the global footprint of a bank's business rises, the complexity of unstructured data and scope of international regulatory and AML activities grow proportionately. Moreover, it becomes a very difficult task for a large bank to detect systematic money laundering activities in unstructured data relying on multiple external data sources, public documents, news feeds, or social media. Further, there are large fines imposed by regulators and reputation loss if they fail to detect any illegal activities. Thus this has led to major banks shifting their focus towards obtaining insights from unstructured data using big data and AI.

In most cases, AML systems work using structured data. In addition, there are many useful insights that can be extracted from unstructured data such as relationship information and new risk events. For the most part, using unstructured data has not yet become an industry standard and most organizations are utilizing third party data providers (e.g., WorldCheck and RDC) to provide clean and structured data. Innovation in this area is coming from larger organizations that can invest the budget and resources in order to explore how new technologies can be used and establish market best practices.

Large firms place a greater importance on understanding their customers better and having a complete KYC profiling. This is largely due to high net worth and high risk individuals, whose profiles need to be understood completely, opening accounts. This leads to having more unstructured data read and collated for the analysts to have a 360-degree view. Process automation saves time and ideally leads to better risk management and compliance. While many small and medium size banks are aware of unstructured data's importance, they are not seen as early adopters in using advanced technologies and generally lag large banks. The smaller firms are more likely to use the solution as 'out of the box' to meet their compliance needs. Generally, such firms find it difficult to monitor unstructured data in view of the complexities and associated efforts/costs.

## Change drivers


In the next few years, some of the main drivers for the AML industry will be technological developments, cost pressures, and regulatory changes. Out of these, we will deal with regulations in the next sub-section, and the rest of the factors here. As the awareness around AML increases, large companies are expected to expand the reach of their financial crime programs and cover areas such as anti-corruption practices.

The increasing requirements and growing transaction volumes will lead to a more complete integration of analytic capabilities and visual analytics to allow for additional insights into the AML related issues being tackled by firms. A more robust AML program of this type would allow firms to maximize their profitability and competitive advantage by allowing them to sell products that would be too risky to manage otherwise.

The cost of compliance has been rising steadily over the last decade. It has forced financial services firms to be more efficient and productive in managing their operations. Firms are handling their AML transaction monitoring and workflow capabilities with the objective of reducing the cost of compliance. Cloud and Big Data computing offer a path to reduce cost while maintaining effectiveness. Updated data architecture across the enterprise, for example, introduction of data lakes. It also requires the modernization of the platforms to allow for in-memory, massively distributed open Big Data Architectures. Improving cost efficiency is achieved by continuous investment and innovation in technology. If these factors are managed well, the industry has the potential to mitigate the risk emanating from the rising cost of compliance.

The use of AML programs has been mandated for more than a decade now. The early adopters of AML systems, including some large banks, are currently dealing with technology that is older and more difficult and costly to upgrade. These firms have to replace their older systems to ensure that they address current requirements and can effectively tackle future challenges. Big-data enabled analytics, neural network, predictive algorithms, AI capabilities, robotics, and pure digitization are among the recent technology that AML systems have incorporated. Unstructured data analysis, which refers to the ability to monitor and analyze free-text information could impact trade finance operations and uncover relationship information and new risks.

Such advanced systems can have significant positive effects on the AML investigation processes, making it faster, more efficient and cost-effective. The aim of the leading vendors is to provide a robust and highly scalable latest technological solution addressing all business lines under single platform. There is an acute need to introduce such efficiencies in a market with a limited pool of skilled and experienced professionals. Automation of key processes, which are often time-consuming, allows compliance professionals to focus on the most critical risks.



The growing use of cloud based platforms is also becoming more acceptable in the Asian market, with regulators such as Monetary Authority of Singapore (MAS) giving their approval for incorporating cloud services into current AML systems. There are still limits to which cloud technology can be employed, partly due to the concerns about the location of data centers. Most regulators in Asia prefer that data centers are located within their particular jurisdiction to allow for continued access to the data if the need arises.

An important development is the requirement for consolidation of fragmented technologies and vendors to reduce operating risk. In several of our discussions with industry participants, the idea of a universal financial crime solution came up, involving the amalgamation of AML, FATCA and fraud monitoring solutions into a single platform. Such a solution would allow both a more holistic and streamlined approach, saving resources for firms under cost pressures.


Within the Asia-Pacific region, vendors have indicated significant interest from FinTech, payment and remittances providers, and increasingly from corporates that are concerned about bribery and corruption. Additionally, there is increased demand from firms moving into a market that falls under AML regulation. For example, an e-commerce supplier creating its own dedicated payments product. Gaming firms are another new category that a number of vendors have been working with, and this demand is expected to grow further.

## Regulation

Most firms invest in AML systems because of the threat of regulatory sanctions. Many leading banks have been fined globally for failing to have adequate programs in place and must deal with the associated reputational damage. Further, for some firms that were not covered by AML rules earlier, a change in regulation can bring an existing enterprise into the scope of regulation. Firms using AML platforms often have to adhere to global compliance regulatory standards such as BSA, USA Patriot Act, FSA, BASEL III, and FATCA, while being flexible in adapting to local regulations to allow for a 'glocal' model of AML implementation.

Compliance officers have to provide regulators with information such as an audit trail and the frequency with which evaluation of their compliance effectiveness is conducted. Optimization tools are important to ensure the AML models work as intended and that any loopholes are identified and promptly addressed. AML solutions need to remain aligned with evolving regulations and incorporate new requirements into technology solutions. Recent regulatory requirements include understanding the ultimate beneficial ownership of complex corporate structures, and AML model validation and attestation. New tools are required to map out the footprint of a corporate customer across a financial institution.

Regulators are moving towards a more holistic view of financial crime. This will require banks to be more hands-on and provide more meaningful information when reporting any suspicions. Banks will need to move from a previous



“check-the-box” approach, to a more dynamic and proactive mindset. In the future, some of the most important regulatory requirements are expected to be around the issue of financial inclusion and financial transparency. These will include FinCEN Proposed Beneficiary Owner Rules, FATCA, Personal Accountability Regime for senior managers, Sanctions Screening Violations and the associated fines, AML Model Validation and Attestation, and the Fourth EU Anti Money laundering directives.

To take on the role in stopping bad actors, financial institutions will be expected by regulators to maximize their access to the information available on the widest segment of the population possible. This should allow them to expand their markets while enabling more people simultaneously to have access to the financial system. Another critical area will be the comprehensive enterprise wide regulatory requirement to enable financial institutions to manage and address challenges in each stage of the AML process, namely, screening, KYC verification, risk assessment, suspicious activity monitoring and reporting across products, services, and business units. Some of the new areas for regulation include trade based money laundering and terrorism financing, digital currencies, gaming firms, marijuana related businesses, money laundering via real estate, and cyber risk assessment.



# Comparing Leading Providers

To compare the AML vendors for this report, the questionnaires we sent them focused on a few key aspects of their solutions:

**Clients** – We asked the vendors to give us an idea of their clientele in terms of size and composition to help understand the market each firm serves.

**Onboarding** – Each firm was asked to describe the on-boarding process utilized by the AML platform. In certain cases, this function was performed outside the AML system, but most firms chose to internalize.

**Transaction & suspicious activity monitoring** – An integral function of any AML system is its ability to detect suspicious transactions and activity, and the interviews and vendor replies accordingly were focused on addressing the critical features to address this requirement.

**Alert & Case Management** – A key consideration discussing alerts management is the ability of the system to cope with the large volume of alerts that are generated daily. This was one of the important issues we dealt with, along with understanding the underlying alert related functionality.

**Features dealing with local regulations** – While most of the leading vendors have a global presence and solutions capable of handling a wide array of international and national regulations, our focus was on Asia and how each vendor was addressing the specific regulatory requirements.

**Advanced Analytics** – A related feature to transaction monitoring and alert management is the requirement for integrated and advanced analytics. Firms have to manage much higher volumes of transactions and alerts today than ever before. Hence, was an important topic for our discussions.

**Advanced Machine Learning** – Cyber-surveillance, fraud monitoring and AML are some of the key areas where machine learning and artificial intelligence are being used. Our research sought to assess the level of development and preparedness of each solution in this regard.

**Hosted vs On-premise deployment** – Financial services technology is today becoming much more flexible when it comes to platform deployment and this point studied the approach of each vendor regarding the offering of hosted, on-premise and hybrid deployments.

**Flexible System architecture** – With ever growing volumes and rising cost management concerns, it is important for AML system clients to have a scalable and flexible architecture that allows them to adapt to specific needs.

**Scope for customization** – Similar to flexible system architecture, is platform customization. Clients expect to be able to customize the product in accordance with their requirements. Vendors are also aware of this issue and we sought to understand the unique approach of each firm.

**Reducing false positives and negatives** – False positives and negatives are an ongoing concern for clients. AML systems that are able to learn from client experience over time to minimize errors are preferred by user firms.

**Upgrades** – The expected upgrades to each of the platforms gave us insight into the future focuses of each vendor, which direction they are anticipating the industry to move in. This will help potential clients to assess whether the vendor would be able to meet their specific requirements in the future.



Participating vendors then reverted with a written response which was then followed-up with a phone discussion. In each of the following company profiles, we have taken the vendor responses, removed any 'marketing-speak' and standardized some of the language.

The following table shows a comparison of the main IT services provided by AML systems across the leading vendors. In addition, we also provide a ranking of the various vendors covered in the report in the last section.

	Clients	Onboarding	Transaction & suspicious activity monitoring	Alert & case management	Features dealing with local regulations	Advanced analytics	Advanced Machine Learning	Hosted vs On-premise deployment	Flexible system architecture	Scope for customization	Reducing false positives & negatives	Upgrades
ACI	●	-	■	■	■	■	■	●	◐	●	◐	◐
BAE Systems	●	●	■	■	◐	◐	◐	●	●	◐	●	●
FICO	●	●	■	■	◐	●	●	●	●	-	●	◐
Fiserv	●	◐	■	■	◐	◐	◐	●	●	◐	●	◐
Intellect Design	○	●	■	■	■	■	◐	●	●	●	◐	●
LexisNexis	◐	◐	-	◐	◐	■	◐	●	◐	●	◐	◐
NICE Actimize	●	●	■	■	■	■	●	●	●	●	●	●
Oracle	◐	●	●	■	◐	●	■	●	●	●	●	◐
TCS	○	●	●	■	■	■	◐	●	●	●	◐	◐
Temenos	◐	●	■	■	■	◐	◐	●	●	◐	●	◐

Source: Kapronasia Analysis

**Legend:**

- - High
- ◐ - Intermediate
- - Low
- - Present, but difficult to compare
- - Not Available

# Product Profiles:

## ACI Proactive Risk Manager (PRM) for AML

### Product Differentiation

Accuracy of real time actions is critical to ensuring customer service whilst managing fraud. Customers using PRM achieve this balance by utilisation of rule based detection with user configurable enhanced profiles; out of the box. PRM customers can also choose to extend this capability with ACI's scoring engine and custom models to leverage advanced analytics methodologies for application to big data sets.

Other pertinent features of the PRM solution are:

- Workflow management capabilities with rules-based strategies via a comprehensive java-based application
- Real-time monitoring / testing
- Best practice rules available at Implementation
- Enhanced behavioral profiling
- Support for electronic transmission of Government reports
- Configurable rules and queue management
- Link analysis for trend and relationship evaluation
- Optional model scoring capabilities technology
- Custom models to detect risky customer behavior
- Complete audit tracking of administrative, transaction and investigator activity
- Implementation options for quick and cost-effective compliance
- Case management functionality

### APAC specific requirements

Asian regulators prefer the use of an on-premise solution or client's own cloud, not the vendor's cloud offering so the data typically would also have to remain with the client for regulatory reasons. Due to lower levels of awareness about AML systems, the APAC region is more susceptible to being a conduit for money laundering, so the local financial service providers need to catch up. Recent cases of money laundering have resulted in many financial institutions in Asia closely scrutinizing their current capabilities across the board. Not just AML but also recognizing the need to leverage the synergies between both AML and Fraud. Big banks are leading in this process, and need to educate the rest of the industry. For example, India is making some headway in this.

## Key Product Features

### *Onboarding*

PRM is not typically used for on-boarding, but it is possible to attach some rules to an on-boarding tool such as blacklists which can be used for rule detection. It offers a flexible 'Reference Data Manager' functionality, which enables any data to be uploaded, including watch lists, black (sanctions) lists, etc. Fuzzy-logic soundex integrations with phonetic indexation can meet requirements for detection against names in many languages. Exception lists can be created for customers domiciled in a high-risk country. In addition, the enhanced profiling requirements of high-profile/high-ranking government officials or politically exposed persons (PEP) can be monitored. The solution provides the ability to monitor and adjust an individual's degree of risk respectful to the local regulations. Rules can be authored to exercise the exact amount of investigation and review on new or existing customers who are identified as requiring enhanced due diligence and may exceed the risk-tolerance of the institution. Watch lists and customer reference data can be assessed by real-time or near-real time rules, at account opening or in batch review.

### *Transaction and suspicious activity monitoring*

PRM delivers enterprise payments risk management by monitoring suspicious activity, alerting on anomalies and providing visibility into information across customer accounts, channels and lines of business. All activity by a customer can be monitored.

### *Alerts and case management*

PRM offers an alert management solution which provides customers with the ability to define, configure and prioritize the management of a broad range of alert types to help financial institutions manage, track, control and prevent potential compliance events; and detect patterns and gather intelligence to reduce losses from potential fraud events and other activities, such as 'money mule' and account takeover situations. The queue-driven alert manager assists in the collection of relevant information and enforces pre-defined processes. The alert manager provides a central repository for tracking consolidated transaction histories, reporting losses and communicating to external parties.

### *Currency transaction reporting*

Information not available.

### *Features dealing with local regulations*

PRM's client/server component can be implemented to comply with government regulations. This component offers efficient work-flow management capabilities with rules-based strategies at the core. PRM allows the ongoing creation of

additional rules in real time, enabling employees to address evolving reporting requirements, government mandates and new money laundering schemes.

### ***Advanced analytics and network analysis***

PRM offers an analytic scoring engine with a customized scoring model for use in enterprise transaction monitoring scenarios which uses pattern recognition technology to detect fraud and potential money laundering activity.

### ***Machine learning and AI capabilities***

PRM's neural network compares the characteristics of a customer's financial activity with the custom model and recorded patterns of behavior for each account holder. The neural network then assigns a score reflecting the degree of risk for each transaction. This tool complements the enterprise monitoring solution where the use of a scoring model contributes to a risk-based prioritization and alerting mechanism.

### ***Hosted versus On-premise deployment***

Clients can choose between a cloud / on-demand version or an on-site version.

### ***Pricing***

Information not available.

### ***Additional features***

PRM is strong in the transaction monitoring space, including for politically exposed persons (PEPS), blacklist and sanctions capabilities.

### ***System Architecture***

The system needs information in a pre-designated format. Otherwise it has a relatively open architecture. In Asia, a local distributor is required to direct technical work and conversations. The distributor usually takes care of the architecture on the part of the end-client. The solution's input architecture allows clients to add new pieces of transactional data as new channel detection/prevention controls are required.

### ***Library of suspicious transaction types***

PRM combines ACI Analytics, including a library of defined rules, with enhanced behavior profiling for a flexible response to the evolving nature of financial crime.

### ***Product output***

The solution provides pre-built reports, accessible on demand, with a number of configurable parameters to retrieve the pertinent data.

### ***Scope for product customization by client***

Clients are able to configure rules to capture required scenarios in order to comply with regulators, internal / external governance and audit requirements. It is a configurable system, with external application extension points and an open database design which customers can utilize in providing additional reporting, for example, to third parties for AML and compliance reporting requirements.

### ***Reducing false positives and false negatives***

PRM's scoring engine seeks to minimize false positives, allowing staff to focus on the highest risk activity. Investigators are also provided with reasons for the score to improve analysis.

### **Upgrades in the next 3 years**

ACI incorporates insights gleaned from environmental scans of its customer's future needs and technology changes. These insights are used to direct its product roadmap with current focus on building on its existing advanced analytics applications, case management and automation of its regulatory compliance capabilities.

# Product Profiles:

## BAE Systems NetReveal

### Product Differentiation

Some of the important differentiators are:

- Optimization: Machine learning enhanced detection, mirrored sandbox, synchronous data integrity.
- Packaged Big Data: Big Data scale without the setup overheads.
- Enhanced Behavioral Profiling: In memory, parallel performance to cope with Big Data volumes.
- Open Detection Engine: Ability to modify and author new scenarios by end users – ‘white box approach’ to alert generation.
- Integrated risk management: The BAE Systems NetReveal integrated detection and investigation product suites differentiate the solution from competitors’ potentially fragmented solutions. Product design is modular, enabling customers to incrementally add components.

### APAC specific requirements

All regions need to meet AML requirements to compete in a global market. Just as with different tiers of banks, some regions are more mature with subtle differences than in other markets.

### Key Product Features


BAE Systems NetReveal Anti-Money Laundering Transaction Monitoring solution is part of an enterprise compliance suite that includes Sanctions & PEP screening, Transaction Filtering, CDD/KYC, AML Optimization, AML for Correspondent Banking, SAR Filing, Currency Transaction Reporting (CTR), FACTA and Enterprise Case Management. The suite also covers banking fraud including Application Fraud and Account Monitoring, Payment Fraud, Deposit Fraud and Card Fraud.

### *Onboarding*

The NetReveal CDD/KYC solution provides a enterprise-wide approach to satisfy CDD and KYC requirements from initial on-boarding, to ongoing due diligence, to enhanced due diligence (EDD). The Sanctions & PEP solution screens names against watch-lists as part of the CDD/KYC process and ongoing monitoring. Know Your Customers Customer (KYCC) ability allows the client to extend AML monitoring outside of a financial institution as required for "multi-leg" products like Correspondent Banking.

### *Transaction and suspicious activity monitoring*

The NetReveal AML solution employs advanced detection analytics and investigator-centric design to help minimize reputational and regulatory exposure and reduce the cost of compliance. It screens payments against sanctions lists.



Key partners include Dow Jones, Thomson Reuters (World Check) and Accuity (all of whom are list providers). BAE Systems is also a certified solution provider for SWIFT. The solution provides the ability to file suspicious activity reports (SARs) directly from the solution in multiple jurisdictions.

### ***Alerts and case management***

The solution includes case management for initial alert investigation, case management and SAR filing. The case management solution covers all aspects of compliance in addition to fraud and security through one common UI segregated by function and role.

Differentiating features of case management include:

- AML Model Optimization embedded in case management so that end users can optimize AML detection without deep analytical skills.
- Network Link Analysis to expose hard-to-find links in financial crime.
- Enterprise risk management to tie together alerts and cases across fraud and compliance.
- Workflow automation to automate manual steps, streamline processes and reduce human touch points.
- Multi-organization support so that a single instance can support a complex organization which operates across geographic boundaries.

### ***Currency transaction reporting***

The NetReveal FinCEN CTR solution is a stand-alone module that screens cash and cash equivalent transactions and automatically generates and validates CTR reports which can be reviewed and amended prior to being e-filed with FinCEN. Investigators can also create Designation of Exempt Persons (DOEP) cases and the DOEP Case workflow supports the end to end process of creation, annual review and e-filing of DOEP reportable persons to FinCEN via the DOEP Case Initial Case workflow and the DOEP Case Annual Review workflow.


### ***Features dealing with local regulations***

The solution provides out of the box SAR reporting for the U.S. market, with additional support provided to meet the need for country specific regulatory reports. Beneficial Ownership and Sanctions are available out of the box to meet local regulations and can be tailored for the specific regional requirements. Non-domestic tax compliance due diligence and reporting (FATCA) is also available to meet local regulations.

### ***Advanced analytics and network analysis***

The solution provides a standard network analysis tool that visually displays the link between entities, alerts, cases and associated parties. Additionally, as





an add-on component, it offers Social Network Analysis, that can be used to uncover more complex money laundering schemes.

### ***Machine learning and AI capabilities***

Supervised learning is an available option in the NetReveal AML Optimization module. Learning from confirmed true and false positives investigated in case management, a genetic algorithm can suggest improvements to the thresholds of AML detection to improve operational efficiency while maintaining effectiveness. Unsupervised learning is an available option that can be deployed alongside detection scenarios derived from FATF typologies.

### ***Hosted versus On-premises deployment***

On-premises and hosted variants are identical. The hosted variant is deployed on an infrastructure layer provided by an IaaS partner.

### ***Pricing***

Pricing depends on customer size and complexity. For a typical regional bank, 40% of costs in Year 1 are license, 50% are services, 10% support & maintenance.

### ***Additional features***

The NetReveal AML Optimization Module helps financial institutions understand, manage, and improve their anti-money laundering (AML) detection programs, and potentially improve compliance and operational efficiency. The entity resolution feature helps identify duplicate customers to simplify due diligence processes and aggregate risk profiles. Enterprise risk management helps consolidate risk incidents, and not just within the compliance silo.

### ***System Architecture***


The NetReveal AML Transaction Monitoring solution can support a wide range of hardware and operating systems, including traditional on premises data bases, as well as emerging technologies with regards to data lakes. Additionally, it can be hosted as a SaaS.

### ***Library of suspicious transaction types***

BAE Systems provide a number of scenarios and rules as part of the 'out of the box' solution for a customer to begin with which they can then tailor to their needs, or create entirely new ones.

### ***Product output***

The outputs to analysts include alerts, entity information, transaction visualizations, and embedded work-flow to help with disposition. The outputs to



investigators include transaction visualizations, maps of network relationships, alerts, cases, search hits and electronic documents. For regulators, the outputs are in the form of suspicious activity reports and currency transaction reports. For auditors, the outputs include audit logs and model performance indicators. Finally, for managers, the outputs include metrics on AML system efficiency and effectiveness and operational performance.

### ***Scope for product customization by client***

The solution is designed to be utilized as an off the shelf compliance tool that will meet the regulatory requirements of the users. It is a mature product that has evolved to include new and more robust features in each release, with out of the box detection scenarios that can be user modified. In instances where the solution needs to be customized to fit the operational needs of a customer, there is the ability to make changes to the solution to fit that customer's needs. Typically, this is done by the BAE Systems professional services group that will work with the customer to make these changes. Additionally, BAE Systems does work with approved contractors in certain implementations.

### ***Reducing false positives and false negatives***

The NetReveal AML Optimization solution is a module designed to work with the AML Transaction Monitoring solution. It enables clients to manage efficiency and effectiveness of the AML detection process. AML Optimization enables the client's AML Analytics team to simulate proposed changes to AML scenarios, evaluate effectiveness (true positives & false negatives) while also measuring efficiency impact (false positives). It is deployed in a sand-box environment rather than in live production. Any changes made in the AML Optimization console will have no direct impact on any production system. However, a detection model which has been edited within the console can be promoted to production or exported and used elsewhere.

### **Upgrades in the next 3 years**

- Increasing investigation Efficiency
- Data Fusion for improving monitoring effectiveness
- Integrate 3rd party data to improve effectiveness
- Graphic visualization for CDD/KYC
- Visual analytics for detection
- Transactional analysis of movement of funds

# Product Profile:

## FICO Siron

### Product Differentiation

- Holistic GRC approach: any compliance aspect within one consolidated and risk-based platform covering all statutory requirements
- Best-practice research scenarios from more than 1,200 customer installations
- Mitigation of false positive rate (to lower the workload and avoid backlogs of alerts) by self-learning and self-calibrating analytics
- Automatization wherever possible (e.g. automatic elaboration of beneficial owners via 3rd party database, automatic identity resolution etc.)
- Mature configuration (rather than customization): Using a standard solution allows for a low TCO. Thus, upgrading to future versions of the software takes between 2 to 4 weeks
- Easy installation, interfacing and configuration: it takes 2 to 5 months to go live (including any aspect of financial crime detection and prevention).

### APAC specific requirements

There are differences in AML requirements in different regions and countries, ranging from different thresholds and currencies, to different periods to retain data, AML scenarios. The solution has a multi-tenant functionality, which allows for separate “tenants” to be created within the same installation. Thresholds and settings can be individually configured, and users of each “tenant” can only view data from that tenant, while allowing for global maintenance of the system.

## Key Product Features

### *Onboarding*

Siron®KYC provides the capability to enforce compliance policy while improving the efficiency of the client onboarding process. The user can objectively identify those customers that are carrying higher than normal integrity risks. Examples include:

- Established offshore - in which respect attention shall be paid to the FATF's blacklists of NCCT (non-cooperating countries) and other sanctions-, watch- and blacklists
- Politically exposed persons (PEPs)
- Resident in or having funds sourced from countries known or believed to have inadequate anti-money laundering practices or representing a higher risk of corruption
- Suspected to be engaged in types of business activities or sectors believed or known to be susceptible to money laundering

### *Transaction and suspicious activity monitoring*

Siron®AML effectively monitors customer transactions using institute-specific research scenarios, historical information, and peer group profiles to identify money laundering activities. It is a research system targeted to the detection of money laundering and uses a risk-focused approach to the critical task of monitoring for suspicious transactions. The solution applies advanced analytics and scenarios to customer data from all departments, branches and areas of the bank to automatically identify and classify suspicious behavior.

### *Alerts and case management*

All of the Siron modules come pre-built with their independent case managers, but can also utilize a centralized Case Manager Siron®ACM. Alerts are captured in the Case Manager, and compliance users can review each alert, and decide if alerts should be closed as false positives, or escalated into cases. It has the case manager functionalities to add comments, upload attachments, perform close monitoring for suspicious persons, create white-lists, manually create cases, delegate to other users, and many other functionalities.

### *Currency transaction reporting*

The solution case manager provides the regulatory reporting functionality, and users can create Currency Transaction Reporting (CTR) and Suspicious Transaction Reporting (STR/SAR), and upload or send them to the regulator.

### ***Features dealing with local regulations***

Siron complies with the international regulations to fight money laundering and terrorist financing (Third and Fourth EU Money Laundering Directive, USA Patriot Act, Bank Secrecy Act, FATF 40+9 Recommendations). As most countries regulators' policies for AML closely follow FATF, the solution can assist banks to comply quickly, and requires only tweaking of thresholds. Specifically, it implements the CRS-AEOI requirements (CRS = Common Reporting Standard; AEOI = Automatic Exchange of Information) and integrates with customer acceptance procedures and customer base analysis. The system fully covers the CRS due-diligence regulations. Indicators for reportable accounts, such as postal/home addresses, telephone numbers in states with reporting obligations, standing orders to accounts in these states, belong to the basic rule set in Siron® TCR (Tax Compliance and Reporting). Business users may customize and add rules to react to legislative amendments.

### ***Advanced analytics and network analysis***

Siron®AML Advanced Analytics provide advanced capabilities to understand customer behavior shifts, allowing institutions to detect abnormal behavior as well as behavior that is likely to be money-laundering activity. The models use technology such as patented collaborative profiling, behavior-sorted lists and self-calibrating outlier detection algorithms. Siron®AML Advanced Analytics determine and monitor the normal patterns of customer behaviour, and then detect when that behavior changes which can be an indication of suspicious activity. The models can also identify where behavior over time deviates from that expected based on "Know Your Customer" (KYC) information, which has been captured during on-boarding as well as across the customer lifecycle.

### ***Machine learning and AI capabilities***

FICO's AML analytics are powered by data-driven machine learning algorithms and a set of patented artificial intelligence IP. Machine learning lets the analytic model discover these normal patterns and deviations, and helps automate the process of keeping the KYC databases up to date. By approaching transactions and customers holistically, the process is potentially more accurate and efficient than manual segmentations and rules creation for specific changes (e.g., thresholds on foreign transaction amounts).

FICO also involves the AML Threat Score, that is designed to identify customers whose transactions have a high likelihood of suspicious money-laundering activity. The AML Threat Score uses FICO's Collaborative Profiling technology, as well as other FICO analytic technologies and machine learning methods (including neural networks), to learn predictive characteristics that distinguish normal and suspicious transactions. The AML Threat Score is trained on historical data including Suspicious Activity Reports.

## ***Hosted versus On-premise deployment***

The solution can be implemented on premise, and on FICO's Analytic Cloud utilizing Amazon Web Services (AWS).

## ***Pricing***

FICO provides a onetime license price which is based on the balance sheet total and the number of customers of the organization. The license is for unlimited users and environments for an institution. A multi-client license is available for data centres and service providers. As an alternative, a term license, ASP, SaaS can be offered.

## ***Additional features***

Siron®RAS is FICO's unique Risk Assessment tool. It meets the statutory requirements and helps the compliance/anti-money laundering officer to create, continually monitor and update company-specific risk analysis. The solution stores the results of the analysis in a database and facilitates the comparison of the different risk factors. This provides a basis for a qualitative, transparent, and consistent risk analysis. Its work flow guarantees that risks regarding money laundering, financing of terrorism and fraud can be categorized and assessed.

Siron®Risk & Compliance Cockpit (Siron®RCC) provides Compliance Officers with an overview of compliance measures that prevent financial crime. Compliance Officers receive a picture of the efficiency and the risk situation of the entire Compliance organization – for all subsidiaries and countries. Siron®RCC helps financial service providers visualize and control the measures to reduce risks in the fields of money laundering, risk analysis, financing of terrorism, and fraud.

## ***System Architecture***

The solution can integrate with existing systems, such as core banking, SWIFT Alliance Access, etc., and can be installed on wide range of hardware and operating systems, such as WIN, LINUX, etc., and supports varied databases including such as MSSQL, Oracle, DB2.

## ***Library of suspicious transaction types***

FICO provides a library of suspicious transaction types and scenarios for reference. These are simple to configure, and this can be done in a very short time, usually taking not more than a few minutes.

## ***Product output***

The AML hits and alerts can be accessed by Compliance users from the Case Management interface.

### ***Scope for product customization by client***

As a best-practice policy, FICO does not recommend any customization; instead, Siron can be configured to meet the requirements of all the users. Training is provided during the project phase, and includes training for compliance users, and technical system administrators. Train-the-trainer methodologies are used, and FICO recommends active participation from the client team to maximize knowledge transfer. As the Siron system is user-friendly, the level of technical ability to manage the system is not high.

### ***Reducing false positives and false negatives***

There are many ways that Siron can reduce false positives:

- Multiple matching criteria with watch-list/sanction-list data
- Business Rules for pre-check, or post-check, that can be used to filter data
- Health check periodically to fine-tune system
- Whitelists and stop words
- Combination of fuzzy settings
- Different % for different lists for different inputs
- National ID / passport to be identical
- Birth year is different

False negatives are minimized through its scenarios and algorithms, and settings that allow for thresholds to be changed. The design is to ensure that alerts that should be picked up are correctly flagged. It uses these tools and is fine-tuned to be efficient (low false positive) and accurate (low false negative).

### **Upgrades in the next 3 years**

Advanced analytics and machine learning are among the key functionalities that are being upgraded for Siron in the next 3 years.

# Product Profile:

## Fiserv

### Product Differentiation

- Ability to react in real-time
- Clients empowered for detection
- Flexible integration of products and data
- Improved suspicious activity detection
- Behavioral profiling of any entity including counter parties
- Strong beneficial ownership capabilities
- Reduces false positives
- Configurable alert presentation
- Simplifies work-flow with comprehensive alert and case management system
- Integrates management and regulatory reporting

### APAC specific requirements

Much of the legislation is similar across regions globally because there are international bodies that come up with the requirements. In Asia, there is more use of cash, unlike the US and Europe. Looking at movement of funds across border due to limitations of fund transfers in China and India.

### Key Product Features

#### *Onboarding*

The system allows for interface with an external onboarding platform for KYC, risk rating, and watch-list screening. 3rd party for identity verification.

#### *Transaction and suspicious activity monitoring*

This is one of the strong suits of the product. The AML Risk Manager offers predictive models built upon analyzing historical data and joining it with the outcomes of the alert and case review to discover non-obvious transaction patterns indicative of risk. These models are targeted to provide deeper insight into compliance risk previously hidden.

#### *Alerts and case management*

Alerts are rank-ordered by risk as calculated by the predictive model and organizations choose the score threshold that matches their risk tolerance, operational goals and capacity to select those alerts that get reviewed.

#### *Currency transaction reporting*

This feature is provided in the AML Risk Manager.



### ***Features dealing with local regulations***

As part of the product, trade surveillance and market abuse is also touched upon for compliance purposes.

### ***Advanced analytics and network analysis***

The data analytics model optimizes alert accuracy, workload and prioritization and demonstrates a transparent data driven risk-based approach to regulators.

### ***Machine learning and AI capabilities***

Machine learning capabilities involve using inference techniques to manage risk. The use of such techniques depends on client requirement and volumes.

### ***Hosted versus On-premise deployment***

Typically, the AML Risk Manager is deployed on-premise in Asia, but there are some hosted solutions deployed as well.

### ***Pricing***

Depends on the type of financial institution using the system. Fiserv employs value based pricing depending on the risk faced by the client organization.

### ***System Architecture***

The system employs a completely open architecture to analyse transactions.

### ***Library of suspicious transaction types***

The library is customizable depending on requirements. The solution has its own library available as well.

### ***Product output***

Flexible reporting engine provided to generate regulatory reports and self-service reports to manage risk effectively. The AML Risk Manager provides a datamart for the user organization to access data. This drives the transparency required by regulator, as clients need to show regulators how they detected various types of financial crimes. There is full transparency on reporting to clients.

### ***Scope for product customization by client***

The product is customizable depending on risks faced, and allows the user to modify as needed depending on their specific requirement.

### ***Reducing false positives and false negatives***

AML Risk Manager uses advanced analytics and a variety of detection techniques. It assesses risk, then uses different risk techniques dependent on type of risk. The platform provides a False Positive Reduction model that scores each alert and auto-closes alerts with a low likelihood of becoming a meaningful investigation, enabling investigators to focus on the highest risk customers and transactions.

### **Upgrades in the next 3 years**

Fiserv is currently focused on improving the system's front-end KYC and enhanced detection capabilities. Risk-scoring is another area that would be emphasized.

# Product Profile:

## Intellect Design Arena AML

### Product Differentiation

Some of the important product differentiators include:

- **Single Integrated Enterprise Solution:** Intellect AML is one single solution catering to KYC Due Diligence, Black List Scanning (Forward and Reverse Scan), Risk Categorization and Transaction Monitoring. All these modules are integrated and the user does not have to log in and out of disparate systems to handle AML compliance requirements.
- **Multilevel Drilldown:** Intellect AML enables inquiry and investigation by the Compliance Officers get a 360-degree view of the Clients/Accounts/Transactions from Intellect AML console itself without having to refer their legacy or other systems for the underlying transactions or account/client linkages.
- **Case Management Module:** Docket management feature available in the Case Management Module allows the Bank to create a docket of all such communication with FIC or the Central Bank or even internal stake holders in the form of Alerts, Emails, Notes, Images, Documents which can be tagged to the respective transaction within the system. This can be retrieved later on from the history tables from the front end forms.
- **Alert Management Module –** This feature enables the Checking Officer to do all activities related to deep investigation of an exceptional transaction right from the time of its genesis until a logical decision is taken to either report it to the regulator or mark it as false positive.
- **SIL (System Integration Layer):** The SIL form the integration layer through which the Intellect AML seamlessly connects with and speaks to the external systems, including the CBS solutions, Card Systems, SWIFT, SMS Gateway, Email servers etc. SIL enables AML to talk to other systems both online and offline.
- **ODS (Operational Data Store):** A powerful module for generation of User Defined Reports by using simple operation as drag and drop. ODS integrates corporate data from different heterogeneous data sources to facilitate operational reporting in real-time or near real-time.

### APAC specific requirements

Global regulators (e.g. FCA, FINRA, MAS, ASIC) are trying to standardize the AML regulations across the globe as local regulatory differs across the different regions. AML regulations being more stringent in UK and US when compared to APAC. In Asia-Pacific, most jurisdictions have their own local sanction list.

Based on Market study, customer inputs, and the regional requirements Intellect Design classifies the overall requirements are into 4 shells - K1 (for Product

Kernel), K2 (Interfaces), K3 (Regional Requirements) and K4 (Client specific Customizations).

As part of regional support the K3 layer is used and K4 is used for customer specific and country specific support. The clear demarcation helps to plug and use the required set of code for any region and country and customer. This helps in regional regulatory and compliance support. For example: regional support for VLC (Vietnam, Laos, and Cambodia), Philippines, Africa, Sri-Lanka, Middle-East, India, Europe and Americas.

## **Key Product Features**

### ***Onboarding***

The complete onboarding process is monitored and analysed by Intellect AML in real time.

The product has in-depth KYC (Know Your Customer) analyses and the data using multiple templates that specify regulatory and internal mandatory data fields, and provides the details of all KYC deficient customers.

The Risk Categorization Module offers front end forms to define three levels of risk grades viz. low, medium and high across various parameters. Once configured, all customers are risk graded and bucketed in any of these three risk categories by the AML system.

The List Management module provides features for the bank to maintain any number of internal and external black/watch lists. It supports multilingual blacklist upload and also provides online search facilities, options to mark false positives and features to exchange data on an online basis with external systems through the interface module.

### ***Transaction and suspicious activity monitoring***

Intellect AML supports suspicious activity detection by applying a hybrid approach through a comprehensive Rule Engine which has various scenarios and thresholds based on simple parameterized values. The AML Rule Engine consists of more than 75 parameterized Rules which cater to almost all types of banking business scenarios. These Rules will generate alerts on exceptions which the investigating officials can view on screen.

### ***Alerts and case management***

The daily data feed utility takes care of the automated data feed of the daily incremental data from source systems to the AML System. Once this data is piped into AML, the various transaction monitoring rules and scenarios configured in the system verify the source data. Any exceptional transaction is routed to an alert queue from where the Bank's User can view these exceptions

and process them further. Thus the AML system helps in a close monitoring of the transactions in external systems.

Another important feature of Intellect AML is its case management tool. On detecting a suspicious transaction, this tool can be used for its due escalations along the organizational hierarchical matrix for their observations, mail exchange, decisions and authorizations. The tool comes with a docket maintenance facility enabling the banks and financial institutions to have the entire history of events tagged to the transaction including image capture that can reside in the system for any number of years.

### ***Currency transaction reporting***

Currency transaction reporting is fully supported by Intellect AML. This report is generated in the desired format automatically by the system based on a reporting threshold parameter.

Intellect AML provide full regulatory compliance and automated regulatory reporting of CTR to FIU/Central Bank. Also, the solution maintains history data within the system for the CTR filed with FIC.

### ***Features dealing with local regulations***

As indicated earlier for regional support the K3 layer is used and K4 is used for customer specific and country specific support. The clear demarcation helps to plug and use the required set of code for any region and country and customer. This helps in regional regulatory and compliance support. For example: regional support for VLC (Vietnam, Laos, and Cambodia), Philippines, Africa, Sri-Lanka, Middle-East, India, Europe and Americas.


Some of the Local regulations that form part of the product are:

- CTR- Cash Transactions Report
- STR- Suspicious Transactions Report
- CBWTR- Cross Border Wire Transfer Report
- Counterfeit Currency Report
- NTR (Non-Profit Organization Transactions Report)

### ***Advanced analytics and network analysis***

AML system use predictive analytics to do customer segmentation and predict a customer behavior.

Customers are classified into different segments based on their behavior (both financial and non-financial). Behavior modeling of customer lays foundation for risk scoring. This helps in setting threshold levels at a customer segment versus bank level. It helps in reducing unnecessary alerts.



Predictive analytics can also be used to detect systematic money laundering. For this, the platform does analysis of distribution of money in past transactions below a threshold level to detect:

- Systematic money laundering
- Ultimate beneficiary in the whole activity
- People involved in the system

### ***Machine learning and AI capabilities***

Artificial Intelligence in AML system help banks in connecting the dots and capturing all suspicious customers and their activities which may pose high risk for banks. It helps in identifying patterns of financial and non-financial transactions of a customer. This pattern recognition gets better with machine learning capabilities and makes AML system smart enough to identify potential fraudulent/high risk activities of a customer.

Some of the patterns which indicate suspicious activity are:

- Changes in customer profile from low risk to high risk and vice versa
- Multiple transactions of small amounts within a short period
- Use of high risk keywords such as donation, gift, further credit etc. in transactions

### ***Hosted versus On-premise deployment***

Intellect AML can be deployed both on Hosted as well as On-Premise. The firm provides a cloud based offering to banks, which ensures TCO reduction, scalability, flexibility, economies of scale, faster time to market.

### ***Pricing***

Intellect Design has a well-defined product pricing framework. Its objective is to evolve a transparent, ready-to use pricing tool that can be referred by sales units, business units as well as partners to arrive at Pricing for Licensing as well as Implementation for Intellect products including Intellect AML.

### ***Additional features***

Another key module of AML is Risk Categorization Module, where the user can configure the various risk parameters. The risk grades can be defined across various parameters such as:

- Constitution of the client
- Products subscribed by the client
- Account sub types
- Country

- Income Range
- Nature of business
- Profession

The system uses these parameters and performs a full scan across all customers and buckets them in any one of the three risk grades, viz. low, medium, high.

### ***System Architecture***

Intellect AML is an open architecture based, pure java based solution. This ensures longevity and scalability. Also, the solution is modular in design, facilitating easy plug in and plug out of modules.

It is available on IBM/Sun/HP/Unix/Jboss/Oracle, thus supported on a wide range of hardware and operation systems.

### ***Library of suspicious transaction types***

The Intellect AML Rule Engine consists of more than 75 scenarios which has various scenarios and thresholds based on simple parameterized values. These rules will generate alerts on exceptions which the investigating officials can view on screen. As the solution is a pure Java solution, it lends itself easily to customization.

On detecting a suspicious transaction, the case management tool in Intellect AML can be used for its due escalations along the organizational hierarchical matrix for their observations, mail exchange, decisions and authorizations right from its inception until such time a logical decision is taken on the case.

### ***Product output***

In Intellect AML the output of extensive library of banking business rules is provided by:

- Prebuilt canned library of reports for internal MIS and reporting requirements and ODS for user defined reports. These reports can be generated on the fly, on demand from the system any time. Reports can be generated branch wise or bank wise, for the current date as also for the back date.
- AML can push the output of its various processes to the interfaced system via API call. For example: If the CBS pass the necessary details of a prospective customer for sanction screening, AML system can do a blacklist check and populate the result in CBS.
- For visual analytics Intellect AML provides various dashboards.

### ***Scope for product customization by client***

As mentioned, the solution is a Pure Java solution and is easily customizable. To carry out these customizations a person need to be technically competent in few technologies such as Java, RDBMS, SQL. Training the end users is quick because the design and language used in the solution is simple, and was developed keeping the end user in mind. For a standard implementation Intellect recommends one week of training each for the Business and Technical Users.

### ***Reducing false positives and false negatives***

False positives are managed by using Machine learning algorithms. Machine Learning is employed to learn from the behaviour of the Compliance Officer as s/he marks an alert as possible suspicious transaction or a false positive. In this supervised learning, these inputs from the compliance officer serve as the training data using which ML can analyse the system generated alerts. It weeds out the alert which are most likely to be false positive, while ensures that no bad transactions are ignored.

Also, a white listing option is available in the system for handling both black/watch list scanning and transaction monitoring, which can be used either at customer level or at the account level to reduce the false positives. Also, the rules can be tuned to attain a most optimum level to avoid generation of inordinate number of false alerts.

### **Upgrades for next 3 years**

Intellect AML keeps pace with the industry demands and customer requirements through its product release calendar and product roadmap policy. The most important roadmap items are:

- Trade Based Money Laundering
- Utilization of Artificial Intelligence/Machine Learning/Natural Language Processing
- Cloud-based AML solutions
- Behavioural Analytics



# Product Profiles:

## LexisNexis Bridger Insight XG

### Product Differentiation

LexisNexis Risk Solutions is bringing science to risk with innovative technology, data and advanced analytics; and it can provide bespoke capabilities, like watchlist screening. The LexisNexis Risk Solutions flagship financial crime compliance product, Bridger Insight® XG, is a platform solution where financial institutions can access its products.

The product differentiators can be categorized as follows:

- Big data technology, called HPCC Systems®, portions of which are open-sourced. HPCC Systems allows the user to process large amounts of structured and unstructured data.
- Vast repository of data.
- Proprietary linking technology that links people to people, and people to businesses.

### APAC specific requirements

Different countries may have slightly different definitions of what constitutes a politically exposed person (PEP), how long a PEP stays a PEP and the level of PEP that should be included within any screening programme. This variance can be mitigated by providing risk data that adheres to the highest common standard and follows the guidance published by recognised authorities in this area. The other area where countries may differ are the industry sectors that fall within the scope of any AML programme.

### Key Product Features

Bridger Insight XG is the LexisNexis Risk Solutions delivery platform for all of the core financial crime compliance products.

#### *Onboarding*

The user solves for the CIP requirements with the identity verification products integrated in the Bridger Insight XG workflow. Among these requirements is watchlist screening, which is done through Bridger Insight XG capabilities using the WorldCompliance™ collection of risk profiles. LexisNexis Risk Solutions provides due diligence attributes for delivering important risk information on due diligence that is required on the customer.

#### *Transaction and suspicious activity monitoring*

The data products are accessible via XML and Batch for integration into any transaction monitoring platform. This simplifies the case documentation task during alert management, hence reducing cycle time for resolution.

### ***Alerts and case management***

Bridger Insight XG offers flexible capability for case management and workflow, thereby facilitating the implementation and maintenance of operational workflows. Through this capability, the users are able to keep all the relevant pieces of information together to demonstrate comprehensive due diligence practices and controls during regulatory examinations. The platform gives users flexibility in how they manage alerts to align with their own policies and procedures. With predefined alert decisions, alerts can be processed quickly.

Alert Management teams are usually challenged to process unplanned volumes of alerts, whether that is a result of a regulatory look-back or a significant update in global watch lists. For this purpose, LexisNexis Risk Solutions offers an Alert Remediation service through a global network of delivery centres, enabling its customers to outsource this function to LexisNexis. Customers of all sizes use this service. Through this service, customers have access to compliance resources whenever and wherever they need them.

### ***Currency transaction reporting***

Not included in system.

### ***Features dealing with local regulations***

The product provides FATCA compliance through data offerings and identity solutions.

### ***Advanced analytics, including Machine Learning and AI, network analysis***

Considerable technology exists within the match-linking algorithms to increase the quality of the AML match. Risk mitigation is core to user strategies, thus these capabilities can be developed on a custom basis. LexisNexis Risk Solutions analytic capabilities include machine-learning capabilities, as well as decision-tree analytics, and other more traditional analytic approaches to optimize matching and false-positive reduction. Its linking technology also enables the identification of associated individuals, which has the power to build out risk assessments beyond target identities.

### ***Hosted versus On-premise deployment***

It offers both options – hosted and on-premise through Bridger Insight XG.

### ***Pricing***

Bridger Insight XG is marketed globally and across all industries. It offers an annual license plus support fees.

### ***Additional features***

The Bridger Insight XG user interface is available in seven languages, including English, Simplified Chinese, French, German, Spanish, Portuguese and Japanese. WorldCompliance data is provided in English and native language of publication (currently covering 57 languages).

### ***System Architecture***

Bridger Insight XG provides system to system connectivity via XML APIs and Batch. The product is available as Software as a Service (SaaS), in the cloud and hosted on -premise

### ***Product output***

All of the product's data offerings are available through online searches, API searches and batch.

### ***Scope for product customization by client***

The platform offers easy options for flexible customization. Training for customization is provided through the LexisNexis Risk Solutions implementation services. Support is provided through its support teams globally. Risk mitigation is core to user strategies, and the product's capabilities can be developed on a custom basis.

### ***Reducing false positives and false negatives***

Some of the features provided include: auto-false-positive reduction rules, accept lists and white lists. LexisNexis Risk Solutions partners with AML Analytics to deliver model validation, fine tuning, and testing and benchmarking of Bridger Insight XG. This way organizations can identify the adequacy of their screening process.

In addition, custom implementations can be applied to reduce false positives by applying statistical modeling algorithms to the input data for customers interested in custom approaches which can be effective, allowing the user to capture the nuances of any lender's risk mitigation strategy.

### **Upgrades in the next 3 years**

In the next three years, the most important focus will be on enabling a multi-tenant AML/KYC screening utility, as well as the increasing application of advanced analytics, including machine learning and AI.

# Product Profile:

## NICE Actimize

### Product Differentiation

Some of the important differentiators include:

- Financial crime platform: the AML solution suite is a part of comprehensive financial crime platform. The shared platform allows clients to add additional risk and financial crime solutions leveraging the same hardware infrastructure, case manager and data mapping.
- The solution suite provides a single view of risk by consolidating information across the organization, and provides investigators with a way to visualize data analytics, leading to faster and accurate identification of risk.
- Advanced analytical capabilities, including a comprehensive library of out-of-the-box expert rules which span across multiple financial services markets. In addition, the solution suite has an anomaly detection engine which allows institutions to identify unusual and risky behavior of unknown topologies.
- The solution suite is designed to empower business users to conduct research and rule authoring tasks without deep technical knowledge, leveraging business-friendly UI, allowing users to write queries and add additional detection scenarios in plain English.
- All of the components in the solution suite are tightly integrated, allowing organizations to centralize their AML processes, get an organization-wide view of risk and centralize their alert management process. A data loopback enriches the solution detection capabilities and understanding of risk.
- The solution's case manager is uniquely designed to meet compliance requirements including SAR filing, ability to maintain a full audit trail of the investigations including emails exchanged with non-compliance team members, 4-eyes review process, built in reporting and research tools and more, to help streamline investigation.

### APAC specific requirements

- Different jurisdictions have different currencies which need to be accommodated, by setting different thresholds when tuning the system. The solution allows organizations to work in a multi-tenancy / multi-currency mode to maintain different thresholds and settings as needed leveraging the same analytical capabilities.
- Different regulators might also have different regulatory requirements, depending on the regime's priorities and progress. Some regulators take a very prescriptive approach, while some encourage organizations to use a risk-based approach. The solution suite covers regulatory requirements from multiple jurisdictions.
- There is a difference in the regulatory reporting structures. The solutions suite supports multiple regulatory reporting standards including US, Canada, UK, Singapore and HK reporting forms.

## Key Product Features

The AML Solution Suite has 6 distinct solutions:

- Suspicious Activity Monitoring (SAM): end-to-end coverage for detection, scoring, alerting, workflow processing, and reporting of suspicious activity
- Customer Due Diligence (CDD)
- Watch List Filtering (WLF)
- FATCA Compliance
- CTR Processing and Automation (CTR)
- Suspicious Transaction Activity Reporting (STAR)

### *Onboarding*

The Dynamic On-boarding module allows financial institutions to enforce on-boarding policies through an interactive and dynamic interview process, making sure all required customer information is collected through a standard process. This model can be deployed as a set of user-friendly, interactive web-based forms or via real-time web services, the model automatizes and standardizes the data collection process by analysing current customer information and producing the next applicable set of questions based on answers that were already captured.

Once the initial on-boarding process is complete, the model performs real-time risk assessment of the new customer and promotes an initial EDD investigation process when appropriate which will capture timely answers and speed up the on-boarding process. There is an audit trail that contains the captured answers and preliminary risk information which then becomes part of the initial risk profile created for the customer.

The Principal CDD Module assesses risk and maintains a risk profile for every customer. The out-of-the-box risk factors are used to calculate an initial risk score based on multiple customer attributes, such as geographies, PEP status and client segments, and flags high risk customers for further investigation. Throughout the customer relationship life cycle, all new or updated data is being assessed by the solution to alert on significant risk changes. Existing and historical risk profiles are saved, allowing institutions to view risk snapshots for the entire length of the relationship.

### *Transaction and Suspicious Activity Reporting*

Nice Actimize has standardized the approach to developing and delivering these forms as part of its new STAR solution. This standardization allows customers to deploy the report more quickly and reduce maintenance and installation overhead effort and cost. The forms' capabilities vary based on regulatory requirements and typically offer e-filing and auto population of transaction information.

## ***Alerts and case management***

Actimize Risk Case Manager (RCM) is a comprehensive alert, case management and investigation tool as is used by every Actimize solution including those provided in the Actimize Anti-Money Laundering Suite. The case manager allows user to streamlined investigation process, providing more in-depth information for analysts and investigators and enabling firms to more effectively identify risky entities and previously unknown instances of risk. The case manager user interface manages the entire alert and case management process, from routing and assigning alerts to performing research to reporting and resolution.

## ***Currency Transaction Reporting***

Actimize CTR Processing and Automation (CTR) provides an out-of-the-box solution for automatic generation and electronic filing of Currency Transaction Reports (CTRs) directly to USA FinCEN, as well as creation and storage of Monetary Instrument Logs (MIL) within an institution. Furthermore, users can define additional policies as required, such as routing certain CTR activities for additional review and defining exceptions, via an intuitive user interface. It streamlines the complex transaction matching, multi-dimensional aggregation, conductor and beneficiary identification, exemption list creation and screening, and quality control requirements associated with US CTR processing.


## ***Features dealing with local regulations***

Information not available.

## ***Advanced analytics & Machine learning***

The transaction monitoring solution deploys a sophisticated anomaly detection engine, that monitors all the accounts and all of the transactions in the institution-including activities that are not covered by any specific expert models - in order to detect unusual and risky behaviour. Using account and peer group analysis, compliance teams can uncover new money laundering scenarios and other suspicious behaviors, and can take appropriate action, while not wasting time on insignificant events.

For behavior profiling, the system learns the typical activity pattern of each account and maintains behavior profiles on customer activities over specified periods of time. This information is referenced to detect anomalies in expected account behavior. In addition, by segmenting accounts into peer groups and dynamically profiling each peer group's behavior, the system studies the typical activity pattern of each peer group and maintains behavior profiles over specified periods of time. Unsupervised machine learning algorithm is supported by creating account and party level profiles which are created and updated based on transactional data. Supervised machine learning algorithm is supported by feeding the results of alerts disposition back into the analytics engine to be added to future analytical calculations. The solution increases scrutiny for clients who had alerts which resulted in SAR submission. Over



the next 12-18 months, Actimize will be focusing on augmenting the solutions existing analytical capabilities with a new set of predictive analytics that are based on advanced machine learning techniques and advanced mathematical models as well as NRA (Network Risk Analysis) techniques, allowing customers to expand their detection coverage and reduce false positive ratios.

New supervised and unsupervised robotics capabilities allow clients to leverage robots to conduct repetitive and time consuming tasks such as evidence gathering, data fetching and consolidation. This is reducing investigation time and labor, and also increasing investigations quality and consistency.

### ***Hosted versus On-premise deployment***

The solution suite is available either as an on-premise solution, hosted or as SaaS deployment. Generally in the AML space organizations prefer to have complete control over the solution and to not share any transactional and client data outside of the organizational firewall. But there is a trend in the market for organizations to leverage private clouds, as well as becoming more comfortable with SaaS deployments. This is especially relevant for smaller organizations as it allows them to “outsource” some of the IT and maintenance overheads.

### ***Pricing***

Typically, NICE Actimize offers two licensing models for its clients, Perpetual Licensing or Term Licensing. For the Perpetual License option, the client buys the right to use the solution for a perpetual period of time and pays an annual maintenance fee. For the Term License option, the client pays an annual fee including the right to use the license and this typically includes maintenance as well.

### ***System architecture***

The solution's technology is designed to be fully integrated into the customers' environment. The solution comprises of a large set of adaptors, physical – connecting to different data-sources, and logical – connecting to industry standard applications. Actimize Analytics Intelligence Server (AIS) has built-in adaptors for RDBMS systems, MQ systems, TCP/IP connectors, legacy files, etc. AIS uses these adaptors and connectors to legacy systems and data in order to generate exceptions and distribute them to the Risk Case Manager.

### ***Library of suspicion transaction types***

The solution has a pre-defined library of 250+ detection rules including logic applicable for banking (retail, commercial, correspondent), securities, insurance, MSBs and gaming. The AML solution utilizes attributes of any transaction, accounts and customers as part of the logic parameters for creation of AML detection rules and scenarios. Within the transaction, attributes such as the transaction type, amount, direction, security type, quantity, country, currency, originating/instruction/beneficiary parties, financial institution and free-text



information are available, out of the box, for use in the detection logic. Customer and account information, such as the type of account or certain high-risk attributes, can also be used within the detection logic. The AML system can be customized in multiple ways, all insuring that the ability to intake future upgrades is not compromised.

### ***Product output***

- In a typical implementation, the client is responsible to manage the ETL process and to make the required data available to the system. NICE Actimize provides a detailed breakdown of the required data and documents how it's being used with the available detection models.
- The data required for AML is typically sourced from multiple sources including organizational data warehouses or data lakes, payment and transactional systems, core banking solutions, on boarding/KYC systems and CRM solutions.
- The system's outputs include the following:
  - Alerts – indicating an issue had been found in the system
  - Database views – available for customers to extract data from
  - Log files – maintained with each solution
  - Dashboards and BI reports – indicating operational status and effectiveness status

### ***Scope for product customization by client***

- The solution suite is extensible and come with a variety of GUI tools, which allow for carrying out most of required configuration without any IT or vendor involvement.
- The core of each product is based upon platform based architecture rather than a “black box” approach.
- The Case Manager module was designed as a template to be configured. Configuration of the Case Manager is implemented via changes to a simple control-tables repository. The Case Manager module dynamically builds its appearance and functionality from its underlying metadata.
- The solution models are provided as “open code,” wherein the client/user can actually “see” the logic, and modify it, as required, using the Modeler tool.
- The solution offers flexibility in configuring, tailoring and fine-tuning the solution to the user's specific requirements. The modelling tool is not limited to creation of business rules and is used to defined new sources, create new Meta data etc. The modelling tool delivers flexibility to the clients. The solution's Designer Tool is used by business users with the appropriate permissions to define workflows,



either updating the out of the box workflows or creating new workflows for different business processes.

### ***Scope for customization by client***

Information not available.

### ***Reducing false positives and false negatives***

The solution suite provides a number of methods to assist in minimizing false positives and false negatives.

- Profiles, white-lists, and automatic risk reduction when transactions are marked as false positives.
- Profiles are one of the most powerful tools in fighting false positives. As a customer or account's behavior "drifts" over time, the profiles encapsulate those changes in behavior, minimizing false positives and providing "personalized" detection.
- The solution provides detection performance reports to help identify detection logic where there is performance degradation. This enables a "supervised" revision of rules and models to ensure any changes in detection logic are well understood and tested to avoid unintended consequences.

### **Upgrades in the next 3 years**

- Advanced analytics: to augment the existing solution analytics capabilities, improve alert effectiveness ratio and support responsive and dynamic AML programs. This also includes applications such as automated tuning, which will make the tuning process more adaptive to new topologies and trends and suggest to the organization with new optimized configuration.
- Data consortium: to bring industry best practices and benchmarks to participating organizations in order to help improve their detection, improve compliance programs quality and reduce operational costs.
- Simulation: continue to enhance the existing functionality by adding more robust sandbox and simulation capabilities.

# Product Profile:

## Oracle Financial Services Anti-Money Laundering

### Product Differentiation

Some of the important differentiators are:

- Transaction monitoring scenarios and KYC risk models to achieve regulatory compliance.
- The solution encompasses the entire gamut of compliance and is also extensible to cover Risk, Performance and Customer Insight areas.
- It emphasizes data and comes out-of-box with large number of data quality checks. This helps banks to work with a smaller number of false positives and also provides more accurate results to the regulator.
- Manages false positives and achieves operational efficiency with standard, built-in product features.
- Standard product support for local regulatory requirements for SARs and STRs.
- Easy to configure scenarios and risk models to achieve independence from IT and vendor resources.
- Correlate alerts from multiple sources to form an AML compliance hub.
- Accelerated time to market for any component of the FCCM platform.
- Optimal pre-built data environment for persistence and provisioning for any FCCM application.
- Provides efficiency and higher cost savings, is pre-integrated with Oracle Financial Services Anti Money Laundering and Oracle Financial Services Fraud, and utilizes sophisticated information exchange formats to easily maintain and share data across systems.
- Pool of trained and certified AML specialists to guide implementation process.
- Proven implementation methodology with efficiencies derived from multiple complex deployments.

### APAC specific requirements

Oracle's AML scenario library is designed to be configured both along lines of business and geography. Country A and Country B may be running the same scenario, but they tune the scenario parameters to cover widely different product types, transaction types, and threshold values that are specific to their region. It comes with a Scenario Manager tool that helps banks to build their own scenarios as well to meet specific needs of the local regulator OR to address a typology that is specific to their data sets. Also, in the Asia Pacific

region banks are using the Real Time customer screening feature while onboarding new customers.

Oracle Financial Services Anti Money Laundering also supports country specific watch lists. A geography or entity that is high risk to one country may be considered less risky by another. Larger financial institutions can have multiple countries running in the same instance by assigning risks based on their requirements and allowing monitoring at their desired risk levels.

## **Key Product Features**

### ***Onboarding***


The solution offers full KYC functionality that leverages out-of-box integration with other Oracle products like AML, Fraud, and ECM. It offers pre-built risk models utilizing the Oracle Financial Services Inline Processing Engine (IPE), and financial institutions can extend risk models via configuration. In addition to supporting a real-time account on-boarding risk model, it enables continuous due diligence through risk models focusing on periodic re-reviews and accelerated reviews. This includes factoring in identity verification through 3rd party integration, watch list screening and risk-rating against multiple parameters which can vary based on whether they are an individual or legal entity. Another feature of the AML and KYC modules is that they are interlinked.

### ***Transaction and suspicious activity monitoring***

The solution offers a library of pre-configured, out-of-the-box AML scenarios across all lines of businesses to meet regulatory requirements. This library of 100 scenarios is focused across entities such as Accounts, Customers, Correspondent Banks, Households, External Entities, and Addresses and provides coverage of most AML red flags. The scenarios operate on a Financial Services Data Model that is coupled with core banking system structures through a common staging area, ensuring coverage across a multitude of banking products and transaction types. Built-in data quality checks ensure that monitoring is being done on clean data, providing the high-quality results. It helps reduce false positives and decreases implementation time and effort by using models (scenarios) that have been designed with precise parameters and are performance tuned before deployment. This empowers management with comprehensive documentation for each scenario for transparency into behaviour detection logic and process.

### ***Alerts and case management***

The AML solution utilizes an alert management interface that enables analysts to prioritize work and see relevant data pertaining to why an alert was generated. Alert Management has an out-of-box workflow with 4-eyes approval and configurable actions that lead to the disposition of the alert. It can take in alerts and events from third party systems as well, providing a single interface for triaging



and resolving alerts. Alert Management is fully integrated with Oracle Financial Services Compliance Regulatory Reporting as well as Oracle Financial Services Enterprise Case Management. The Enterprise Case Management module, while integrated with Alert Management, can also be utilized standalone. Enterprise Case Management supports client configured workflows and processes. It enables financial institutions to consolidate investigations for anti-money laundering, know your customer, fraud, and foreign account tax compliance act (FATCA) compliance on a single, enterprise platform. The Enterprise Case Management module is integrated with Compliance Regulatory Reporting.

### ***Currency transaction reporting***

Oracle Financial Services Currency Transaction Reporting fully manages all aspects of US currency transaction reporting and provides CTR reports within a single, unified platform, enabling banks to manage the current transaction reporting process and gain a 360° view of all daily cash activities. It supports the detection of CTR activity, due diligence and '4-eyes' approval workflow for ensuring completeness of data and the creation of efiles for e-submission.

### ***Features dealing with local regulations***

Oracle Financial Services Foreign Account Tax Compliance Act Management is designed to address immediate and long-term compliance. The application minimizes impact to current operations and architecture by providing best practice U.S. compliance expertise through pre-configured yet configurable FATCA account categorization, due diligence, and reporting capabilities. The Common Reporting Standards module is designed to support a financial institution completing and filing CRS reports to applicable regions.

### ***Advanced analytics and network analysis***

The solution utilizes link analysis algorithms to detect previously unidentified networks using attributes of customer and account data and transactional activity between unrelated parties. These networks form the basis for the ML Network of Account and IML Hidden Relationship scenarios. Additionally, Oracle Financial Services Anti Money Laundering and Oracle Financial Services Enterprise Case Management offer the ability to generate ad-hoc networks against alert, case and current business data.

Oracle Financial Services Crime and Compliance Management Analytics offer business intelligence and analytical reporting, providing clear operational visibility into a financial institution's compliance program performance. Preconfigured reports and dashboards assist in the researching of issues and understanding of how well a financial crimes program is operating. Financial institutions can assess operational and productivity information provides opportunities to enhance business process and realize efficiencies.

## ***Machine learning and AI capabilities***

Oracle Financial Services' Financial Crime Platform allows for Machine Learning and AI capabilities to be leveraged in several areas or stages of processing. Machine Learning in the core detection flow involves:

- Customer Segmentation: Scenario rules (to detect activities that are potentially interesting from an AML perspective) are run with different thresholds for different segments of customers and accounts. Customer segments are defined through expert knowledge and bottoms up customer clusters discovered using machine learning.
- Event scoring: Incoming events will be compared to scenarios and scored (prioritized) based on past history of how important similar events were, i.e., past history of case investigations is used to create machine models to predict the importance of new events.
- Event Graph Scoring: Related events are combined into a Graph (or network) and the network itself may be scored for importance. This is a combination of graph analytics and machine learning. High scoring graphs of events are then promoted as cases for investigation.
- Pattern Detection: Machine models may be employed directly on transaction data to detect suspicious activity and AML patterns.


Machine Learning and Robotics in the Investigation Flow involves:

- Next best Action: Speeding up case investigation is a key requirement. By learning from the sequence of actions taken when adjudicating past cases (what actions were performed for a particular type of case in the case management system), the model may be used for predicting what is the next best set of actions for a new case.
- Robotic Process automation: Much of the investigation process involves doing repetitive tasks. Robotic process automation software may be employed to automatically perform such tasks.
- SAR Narrative Generation: Much of the content of the Suspicious Activity Reports may be generated using Natural Language processing / robotic techniques. SAR narratives can be created using text analytics models.

## ***Hosted versus On-premise deployment***

Currently the Oracle Financial Services Financial Crime and Compliance Management (FCCM) suite of products can be installed on a dedicated cloud infrastructure for the customer in an IaaS or PaaS settings. Oracle can additionally perform the installation, configuration of FCCM products and continue to maintain it for the customer with a Managed Services offering.

There is an emerging appetite for cloud offerings which are designed to automatically provision and be self-managed in SaaS type settings but these



are currently limited to ancillary units of functionality around the core FCCM transaction monitoring. For example, alert or event optimization, and analytics. These are geared to primarily help optimize and manage change to the core transaction monitoring systems.

### ***Pricing***

Information not available.

### ***System Architecture***

The AML system is built on open architecture principles designed to plug and play with existing systems. There are many instances where the Oracle Financial Services Anti Money Laundering solution is used for transaction monitoring but a different system is used for case management and vice versa. It supports the all popular versions of hardware and operating systems such as Intel/AMD based hardware to Linux/AIX for operating systems.

### ***Library of suspicious transaction types***

Oracle Financial Services Anti Money Laundering has a library of around 100 scenarios that cross multiple red flag activities and focal entities. It is configurable. Each scenario contains multiple parameters which can be tuned as threshold limits on an institution by institution basis. Additionally, even within an institution these sets of thresholds can be further segmented along geography, lines of business, risk, types of transactions etc.

### ***Product output***

The data is part of an open data model. It can be accessed via standard database tools. From a visualization perspective, it can be queried from within Oracle Financial Services Crime and Compliance Management Analytics. And it is viewable and searchable as part of alerts or cases.

### ***Scope for product customization by client***

Oracle Financial Services Anti Money Laundering workflows can be updated and configured by administrators with basic SQL skills. Oracle Financial Services Anti Money Laundering user interface can be updated with moderate level training on Oracle Financial Services Analytical Applications Infrastructure forms framework (UI changes primarily involve XML updates). Tuning of scenarios, setting of assignments and scoring use a standard web UI, requiring no particular technical skills.

### ***Reducing false positives and false negatives***

Oracle Financial Services Anti Money Laundering uses a combination of data preparation techniques and a unique matching processes to arrive at accurate match results and reduce false positives. These are described in detail below:

**Adequate Data Preparation:** The data preparation steps address these common errors in data and cleanses the data before the matching process. The solution employs techniques such as transliteration to convert from one writing system to another using character-level rules.

The solution also uses transcription and variant matching for more complex languages (such as Arabic) to identify all potential name equivalences. Techniques such as profiling, auditing, transformation, and text analysis are also used to validate data, remove white spaces and possibly erroneous characters, or split a single name field containing multiple attributes into several fields. These capabilities enable organizational data to be optimized to match rules.

**The matching process:** The solution enables business users to define the rules that determine which records are matching. A granular comparison of records, along with the use of match patterns, takes the best of multiple methods discussed above but still incorporates user-defined rules. The following four steps within the matching process are explained in more detail.

- Assign match keys: Match keys can be used to provide high-level matching. This enables similar records to be grouped for further comparison. Multiple match keys (built from different components) are generated to ensure matching records will be clustered together.
- Cluster records with common keys: All records that share a common Match Key are clustered together. When multiple keys have been generated for each record, the record can appear in more than one group. This significantly reduces the chances of false negatives.
- Compare records: Each record in a cluster is then compared to every other record in the cluster. Comparisons are carried out at the field level, with each comparison producing a result according to a defined business rule or a probabilistic score. Together, the results for each comparison build a match pattern for the whole record comparison.
- Match rules: The resulting match pattern is then validated against the user-defined business rules which detail the combinations of field level results that can be considered a definite or potential match. The results can also be ranked according to the institution's risk profile with potential matches flagged for manual review.

By tuning these rules to their own data and risk profile, financial institutions are able to control the screening process.

## Upgrades in the next 3 years

- Improve monitoring systems
- Core AML transaction monitoring and workflow capabilities
- Enhance case management productivity



# Product Profile:

## TCS BaNCS

### Product Differentiation

The factors below differentiate the TCS BaNCS solution from its competitors.

#### Screening:

- List-agnostic facility permits management of an unlimited number of lists
- Screening against Sanctions, Embargos, PEPs (Dow Jones, WorldCheck, Factiva, Lexis Nexis), and internal lists
- False positive management through innovative text transformation techniques

#### KYC policy check:

- KYC policy engine to cover global regulatory environment (BSA, BASEL III, Third and Fourth EUMLD, USA Patriot Act and Dodd Frank Act)
- Flexible policy engine to accommodate local regulations
- 360° case profile creation and management

#### Risk Analyzer:

- Profile based risk assessment
- Dynamic behaviour based risk assessment

#### Activity Monitoring:

- Pattern Analysis based on FATF and other regulatory guidelines
- Link Analysis to unearth hidden networks
- Monitoring of behavioural deviations

#### Case Manager:

- Detailed drill down justification with related alerts and cases to make informed decision
- In built configurable dynamic workflow covering end-to-end process steps
- Centralized-Decentralized setup to provide overall control and scope

#### Report Manager:

- Complies with current global regulatory reporting standards
- Flexible reporting engine to accommodate local reporting standards
- On-demand access to management reports
- Dynamic report builder to assist users in creating own reports

#### Technology:



- Compatible with Oracle , DB2 and PostgreSQL databases.
- Designed in Responsive framework
- Multi lines of business integration with a single product installation
- Real time and batch mode of integration
- Scalable for higher volumes
- Multi entity & Multi Lingual Support

## APAC specific requirements

FATF lays out the recommendations that need to be complied for AML across the globe. The geography specific AML regulations by the Financial Intelligence Unit (FIU) are largely dependent on the FATF recommendations. The extensive rule library that is available in the product complies with all the 40+9 FATF and other geo specific regulations, making TCS BaNCS a fit for most of the regulations laid out in specific geographies. However, for rules that are unique to the FIU or the financial institution due to the local nature of business, the base product upgrades are integrated into the geo specific versions. This makes the base version of the product universal and ready to use for a large customer who has operations across multiple geographies.

## Key Product Features


### *Onboarding (including KYC and identity verification, risk rating, watch-list screening)*

TCS BaNCS is built with a configuration module where rules for KYC customer/ account verification, risk rating, FATCA/CRS check and watch list screening are configured. During the onboarding process the solution can be integrated with source systems in an online mode using Web-Services to screen the customer, verify the required documents as per the organization's KYC process and also determine the possible risk level of the customer based on profile parameters such as occupation, annual income, nationality etc. The application can also integrate in batch mode using XML and CSV interface to perform back book review and generate alerts for the analysts to perform due diligence.

TCS BaNCS is capable of triggering alerts when any declared attribute of any customer is altered over time such as DOB, ID Number, nationality etc., when there is a risk movement and when updates to sanctions' list generates a match to existing customer for analysts to review. The attributes which need to trigger such an alert for KYC purposes can be configured by the business end-users directly.

### *Transaction and suspicious activity monitoring*

TCS BaNCS is built with a configuration module and rule templates to satisfy global transaction monitoring needs. Business users can configure the anti-



money laundering typologies using the rules without any IT intervention. The transactions from various source systems, sourced to the compliance application using the standard interface, will be sifted through to verify if any configured anti-money laundering typologies are breached. An alert is generated in such an eventuality for the analysts to review.

The rules can be used to configure complicated typologies such as the fund flow through, occurred event etc. The configuration module lets business users configure behavior monitoring rules, peer group monitoring and also allows dynamic/behavior risk scores to be calculated based on the customer's transactional behavior. Suspicious Transaction Reports (STR), in both PDF and XML formats as per local regulatory needs, can be generated and presented to users without any IT intervention. Reasons or grounds for suspicion can also be entered which would be used while filing the reports

### ***Alerts and case management***

TCS BaNCS is built with a case management module where all the alerts are generated based on the configured rules can be analysed and action(s) taken. The workflow action, is mapped to the role and access levels of the user and can be configured based on the organizational needs.

The case alert management module provides a 360 degree view of customer behavior and data, for the analysts to review the alerts. User configurable and flexible work flow, which can be modified to align with organization's needs, aids analysts to take actions on the alerts generated in the Case Manager. Multiple alerts can be combined to form a case upload, including supporting documents and external links supporting escalations, to compliance officers for review and approval and/or to file STR's. The case alert management module has in-built workflow features such as auto emails, alert priority, auto alert assign, and alert escalation for those alerts which have breached SLA limits.

### ***Currency transaction reporting***

Specific scenarios for CTR reporting can be configured and transactions which breach the scenarios will be automatically flagged for CTR reporting. The report generation process is automated and the reports generated can be reviewed in the case manager before final submission. Changes to the reports can also be recorded in the dedicated regulatory reports sub module in the case manager. In certain customer geographies, where the local regulator provides integration for report upload, the solution has been integrated for seamless transfer of reports to the regulator after verification and approval.

### ***Features dealing with local regulations***

TCS BaNCS is a full suite that meets the global AML, KYC, Watch list screening needs and with inbuilt modules and rules to meet both the global and local tax regulation needs such as US FATCA, UK FATCA, CRS, HMRC etc. The rules engine is highly flexible and robust, and used to comply with AML and Tax

compliance regulations globally and locally. TCS BaNCS architecture supports building and maintaining new rules and monitoring features to meet any financial institution's needs.

### ***Advanced analytics and network analysis***

TCS BaNCS has the core capabilities to raise a red flag by analysing the data that is being captured. The application is configurable to different capacities of suspicious monitoring. It can detect suspicious activities by applying the following transaction monitoring techniques:

- Threshold and statistical analysis
- Behavior analysis
- Link analysis
- Pattern analysis

Additionally, the system has built-in capabilities to determine the standard deviations of customer transactions as per the Bessel standard, peer network analysis in a group, link network of customers with possible match in their attributes.

### ***Machine learning and AI capabilities***

TCS BaNCS works on a philosophy that DNA fingerprints are unique and the financial nature of every customer is also exclusive. The solution's rich detection capabilities and artificial intelligence attempts to unravel the financial DNA of every customer and create a behavior profile for each customer, which is then used to detect anomalies from expected behavior of every customer within itself or with its peer group. AI capabilities of the solution enables users to analyze and predict the impacts of rule changes before they can be made active. Additionally, the solution is capable of detecting suspicious activities by applying the following transaction monitoring techniques:

Threshold and statistical analysis:

- Behaviour analysis
- Link analysis
- Pattern analysis
- KYC analysis

### ***Hosted versus On-premise deployment***

TCS BaNCS can be deployed on On-premise and in cloud environments.

### ***Pricing***

TCS offers various pricing models to its customers. No additional details.

### ***Additional features***

- Responsive Web Design – Architecture allows the content of the application to render across all screen resolutions of devices such as desktop, laptop, tablets.
- Multi Browser & Data base Compatibility – Ability to render the content of application across multiple modern browsers.
- Enhanced UX – The application UI has enhanced user experience with interactive charts, multi theme support and improved UI with features like quick view, 360 degree Customer Details, Wizard for multi-step.
- Enhanced Security – The application is analysed by Fortify SCA tool to address security risk vulnerabilities (including OWASP Top 10). CSRF protection is provided to the application.

### ***System Architecture***

TCS BaNCS is built on open architecture, which can integrate with various source systems. TCS BaNCS exposes standard interface formats for both batch and online integration. For online integration of the application with various source systems, web services are exposed for consumption by external teams. For batch mode of integration standard interface formats are available for various source systems to consume.


TCS BaNCS is hardware and operating system agnostic. It supports deployment on various OS such as IBM AIX, Sun Solaris and Oracle/HP/RHEL Linux platforms. The application has also been deployed on different hardware stacks such as the IBM Power series, Solaris Sparc, Intel, HP, Exadata platforms and different storage hardware such as the ZFS storage, 3 Par, SSD, Flash etc.

### ***Library of suspicious transaction types***

The application has a rules library. A business user can configure any suspicious transaction type based on existing library rules. Application experts accordingly suggest the possible suspicious transaction patterns during the time of implementation. Additionally, it provides the flexibility to modify the patterns and thresholds at any point of time without having any IT intervention.

### ***Product output***

TCS BaNCS integrates with various source systems in both batch and on-line modes for customer, account and transaction data. The results of analysis of this data, based on the rules configured by the compliance officers, trigger alerts in the case alert management module for investigation officers to analyse. The application is also capable of integrating with external mail servers and/or use the in-built mail feature to trigger mails to the configured analysts whenever an alert is generated.



TCS BaNCS is built with user friendly, responsive GUI where the investigation officers can analyze alerts and obtain 360 degree views of customers. The information can be used by the analysts to take necessary action and file STR's.

### ***Scope for product customization by client***

TCS BaNCS can be customized to meet the unique needs of different types of financial institutions.

### ***Reducing false positives and false negatives***

TCS BaNCS is built with mechanisms to maintain false positives and false negatives. Whenever any alert is generated, analysts can initiate a record as false positive, which will flow through an approval process (maker-checker) before it commits in to the system.

TCS BaNCS rules and rule algorithms such as name & DOB match, name, address and DOB match, phonetic match, fuzzy logic etc. are built to analyze all facets of customer data before creating an alert, thereby pro-actively reducing false positives. The application is built with token cleaning and token standardization features to enable business users to configure tokens which need not be scanned, and to tokens which need to be interpreted as standard terms, for example Ltd as Limited, etc..

### **Upgrades in the next 3 years**

In the future, TCS will work to aligning the product to the cloud and develop with other technological advances in the market.

# Product Profile: Temenos

## Product Differentiation

The Temenos Financial Crime Mitigation (FCM) product family integrates into any third party core banking system. In addition, it is also available as an integrated solution into Temenos Core Banking (formerly known as T24) allowing banks to experience complete coverage in banking. Temenos' Country Model Bank approach further allows banks benefiting from out-of-the-box rules together with pre-packaged workflows for quick installations. The lexical knowledge base combines matching algorithms for accuracy in hit detection related to sanctioned countries. In addition, Temenos' cloud based SaaS offering allows for low barrier entry AML solution for the financial industry.

## APAC specific requirements

Most of the requirements are based on FATF recommendations completed with local and regional FATF-Style Regulatory Bodies (FSRBs), EU and US regulations. The FCM product family is designed to accommodate regional requirements in cases where the out-of-the-box rules and pre-packaged workflows provided by Country Model Banks need to be adjusted.

## Key Product Features

### *Onboarding*

KnowCustomer Plus (KC+) is a risk based solution to classify financial institution customers' according to their risk profile at the account opening process, which integrates into any third party core banking platform or Temenos Core Banking. It uses a detailed risk matrix dashboard including the risk status, range and count to ensure full customer profile awareness. The system offers flexibility; including the ability to add search criteria filters (at simple, advanced, column, identity, address, country or risk level) or create, amend or delete assessments. It uses advanced algorithms to calculate compliance risk scores of new and existing customers, based on the customer profile.

Temenos' Screen protects a bank's business by screening and accurately profiling customers and all types of transactions on watch lists (including sanctions). Its versatile, risk based approach integrates lists from various origins: public, commercial or private applying geographic and business rules. Screen's flexible workflow framework allows a bank to define roles/access rights, context-based validation and 2, 3 or any number of review steps. With additional complementary features such as sophisticated wizards highlighting enhancements and test lists, a bank has a comprehensive solution for all its screening needs.

### *Transaction and suspicious activity monitoring*

Temenos' Profile is an 'out of the box' anti-money laundering solution. It provides web-enabled, end-to-end customer profiling and transaction monitoring which

integrates into any third-party core banking platform Control is also ensured through flexible configuration as well as an automatic report generator engine and customised reporting reducing a banks data mining costs. Profile's processing and detection engines are simple to configure and use.

### ***Alerts and case management***

FCM's case management functionality supports a bank's specific review process which enables users to further enhance the evaluation process, analyse historical transaction data and identify consistent trends in false positive alerts. The user interfaces are designed for users who work daily with the tool, i.e. efficiency in working with the tool is key. Alerts are presented in full business context.

### ***Currency transaction reporting***

FCM Profile supports the creation of regulatory reports such as Suspicious Activity Reports SAR and Currency Transaction Reports CTRs in a flexible workflow during AML alert evaluation. FCM Knowledge Management allows creation of SAR's as a result of other types of alerts, e.g. Watch List alerts.

### ***Features dealing with local regulations***

FCM is designed to integrate specific regulatory requirements during installation or during day-to-day-operations. This is achieved by a series of configuration files and tables, all of them with default values that can be modified to meet the bank's specific requirements.

A recent enhancement refers to FATF R16 to detect and report and/or stop transactions with incomplete payment information. The FATF R16 modules provides out-of-the-box rules that can be adapted to the firm's specific needs.

### ***Advanced analytics and network analysis***

FCM's Knowledge Management is a module which gives access to all data and tables processed in FCM Modules. Users are able to understand activity statistics including previously performed checks, a history of the review process, true hits and false alerts. In addition, it features a range of standard reports aimed at internal audit, regulatory authorities (Suspicious Activity Reports) and supporting archives and statistical databases.

### ***Machine learning and AI capabilities***

Temenos' VBot supports 'automated evaluation' to reduce the amount of manual intervention. The component allows for accuracy in hit detection and automated evaluation of false positives based on learning from past decisions.



### ***Hosted versus On-premise deployment***

FCM has been designed with a number of deployment options. It can be implemented as a standalone Temenos solution that can be integrated with a 3rd party core banking or payments systems; or it can be integrated with Temenos' Core Banking solution, saving on additional complex technical integration. With FCM Screen's cloud-based delivery model businesses get quick access to Screen without the need for additional internal IT resources and infrastructure. The same offering for FCM Profile will be released later this year.

### ***Pricing***

Information not available.

### ***Additional features***

Stripping & Circumvention is an additional module to detect and stop transactions where suspicious data have been willingly removed to circumvent alerts.

### ***System Architecture***

It is an open system and can be integrated into Temenos' Core Banking solution or any other core banking system from other vendors. Temenos' FCM product family is based on an open architecture and agnostic of hardware and operating systems.

### ***Library of transaction types***

There is an out-of-the-box set-up that can be used by the firm as a starting point for user acceptance tests and to get familiar with the tool. If required Temenos supports firms to define transactions types and to customize the configuration.

### ***Product output***

FCM Knowledge Management allows for detailed analytics on data, transactions, user interactions and system configuration about all available modules. Functions to download data for further analysis or processing as well as pre-defined reports provide a complete view on all data and transactions processed in FCM.

### ***Scope for product customization by client***

FCM can be customized to a firm's requirements. The duration of training depends on the level of detail in which the potential users would like to be familiar with the system and its functions. The training can range from an operator evaluating potential alerts to an expert user being able to configure the entire system.





### ***Reducing false positives and false negatives***

Sophisticated algorithms and highly effective scanning methods deliver the lowest possible false positive rates and ultimate efficiency. The unique combination of algorithms and methods allow to set a higher threshold in fuzzy matching and as a consequence to reduce the number of false positive without compromising accuracy in hit detection.

### **Upgrades in the next 3 years**

AML software will no longer make a distinction between AML and Anti-Fraud, even if the teams within a firm would not merge. Although monitoring of transactions will still continue to be important in AML software, online screening of transactions is an industry driver to detect and prevent fraud attempts.

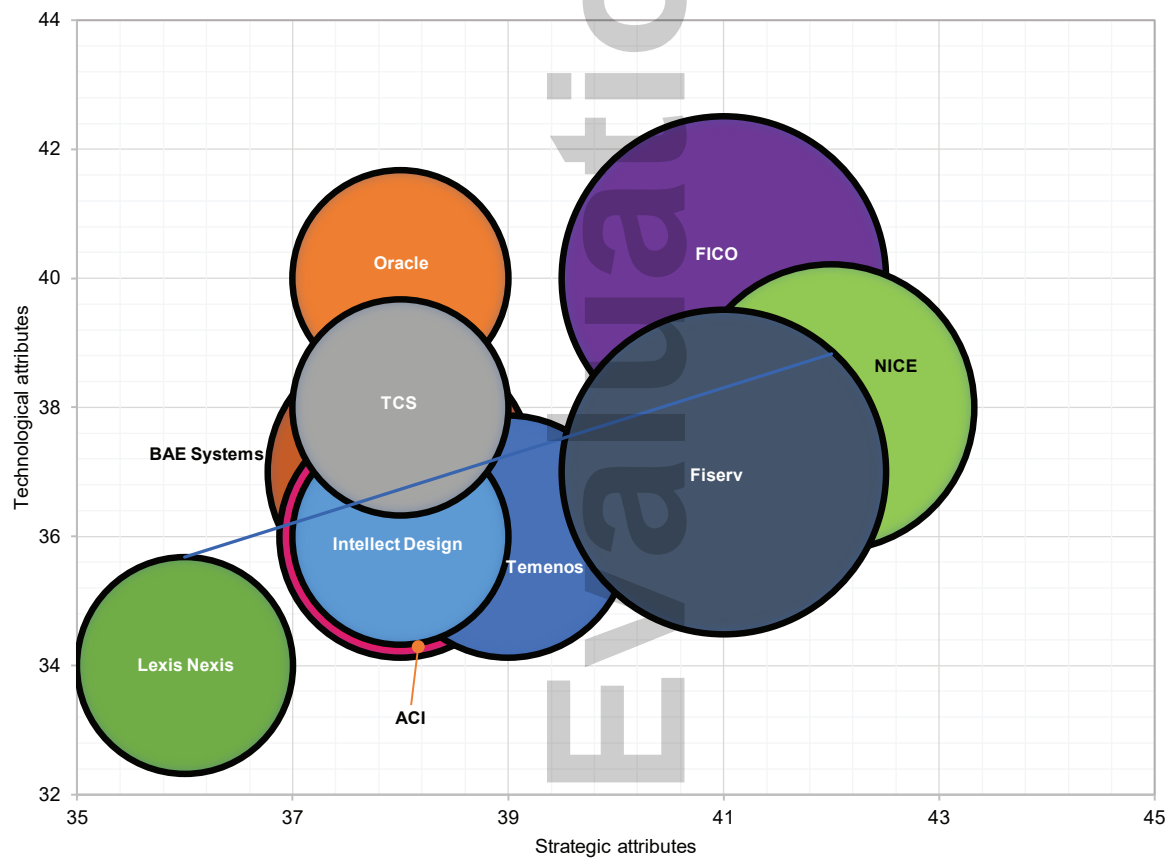
# Kapronasia Competitive Index: AML Solutions

We have compared the leading AML solutions in the Asia-Pacific across two sets of parameters: strategic and technological. The strategic parameters or attributes include firm presence globally and specifically within the APAC region, the holistic nature of the product, the specialized AML functionality within the product, and the product pricing.

The technological attributes include flexibility of deployment, advanced product functionality, machine learning and advanced analytics capabilities, and openness of architecture & ease of customization. The size of the respective circle for each firm indicates the number of clients the firm has in the Asia-Pacific region. Where this number has not been directly provided by the vendors, we have made estimates from our discussions and secondary research.

Table- 1 below shows the overall comparison between the various firms using the strategic and technological parameters. Some of the leading firms across the two parameters include FICO, NICE, Fiserv and Oracle. However, Lexis Nexis did not necessarily perform poorly in the comparison because it serves a slightly different product segment within the AML industry compared to the other vendors.

Kapronasia Competitiveness Index



Source: Kapronasia

# Conclusion

Asia is a fast growing region that has seen financial transaction volumes and international trade boom over the last few decades. Along with the growth of financial services, we have also seen a rise in the levels of financial crimes, especially money laundering. The move towards digital payments across the region has also changed the manner in which money laundering occurs, and it is becoming more difficult to trace it when money is flowing across several jurisdictions in a small period of time.

For larger financial services providers, this requires a change in approach towards AML. From a touch intensive approach that involves each alert being investigated, firms are now moving towards a case-building approach that requires alert or event aggregation, with the initial process being automated and human investigation occurring only once a case has been created to deal with alerts that have a high probability of being an instance of money laundering.

There is a creative tension at play here, since regulators are still in favor of a high touch approach that does not support a high degree of automation in investigation and closing of cases. So market participants have to balance the tools becoming available to them due to technological advancements with the regulatory constraints they face. The cost implications are also an important aspect to keep in mind, since a significant proportion of the costs of using and maintaining AML platforms are labor costs. Hence, firms in highly regulated Asian markets could find themselves to be at a disadvantage competitively vis-à-vis their global counterparts if they have to maintain a much higher human component in AML systems.

The rising sophistication of financial crime, especially money laundering, has led to a spate of recent regulations. Asian regulators are using a 'glocal' approach, with global cooperation for AML being complemented by national regulations meant to take the local requirements of each market into account. The relative maturity of each regional financial market also plays a factor in how the regulator calibrates their AML policy and strategy. Markets such as Japan, Australia, Singapore and Hong Kong are considered to be the more advanced when it comes to financial services, with other fast-growing large markets such as China and India seeing a lot of activity. From the point of view of banks and other financial services providers, along with the AML vendors, operating across national jurisdiction requires a more varied AML approach than we would expect in the European or North American market.

The rise of financial crime related to terrorism and drug and human trafficking has meant that the stakes are quite high. In this context, an important area of recent focus for the Asia-Pacific region has been the possible use of trade financing for money laundering. Regulators and banks both expect the latest AML systems to incorporate capabilities that allow them to keep tabs on possible instances of money laundering in cross-border trade.

While advanced machine learning is playing an important part in helping financial services firms meet their AML needs, cloud services are another way in which AML vendors are making AML systems more accessible for smaller firms and

cheaper to use for larger ones. In Asia-Pacific, there is a growing comfort with use of cloud services, but the region is a little behind the US and Europe and there is still some way to go before it becomes commonly employed. Regulatory concern plays an important part here as most jurisdictions have strict rules governing where the data centers related to cloud deployment are maintained. There are similar reservations with the possible use of utility type models for KYC and AML that are coming up in some parts of the world.

Singapore is an important regional player for AML regulations. Its role as a leading financial center has meant that it has led the way for new AML rules and strategies. But there are other notable countries as well. The leading global role played by China in use of technology in financial services, especially payments, and the push towards digitization of financial services in India, are going to be major drivers in the greater adoption of sophisticated AML software in the region. As financial services becomes more digitized and automated in Asia, it will lead to continued efforts for more sophisticated AML platforms, and we believe that the next few years could be quite exciting in how the advances in technology allow us to modernize and strengthen the AML systems on offer.

A leading European bank recently paid millions of dollars in fines to the US Federal Reserve. It was accused of not declaring properly transactions worth billions of dollars undertaken by its European affiliates. This allowed Russian firms to launder around US\$10 billion through the bank between 2011 and 2015. Similarly, in another instance the bank also engaged in mirror trading that involved buying shares in Russian securities and then selling shares worth an equivalent amount in London. This allowed the clients it traded with to launder their funds. In such instances, it is difficult for AML solution to be able to detect the illegal activity, since the bank itself is engaging in money laundering and fraud. However, for instances in which banks do not engage in the activity themselves but are interested in catching such crime and reporting it to the regulators, AML solutions are an important way of dealing with the problem.

We have looked at the important trends and developments in the space as well as the functionality and features of the leading AML products in the Asia-Pacific. While each solution is unique in how it deals with the requirement for AML, there are some interesting common features that we can dwell upon. The first is the ability of almost all vendors to offer different types of deployment, including on-site or software as a service (SaaS). Some firms were more sophisticated as they also had a hybrid solution that combined features of different types of deployment for different parts of the same solution. But most firms have shown awareness of the fact that as they reach out to users of all types and sizes, they need to be more flexible in how they deploy the solution.

Similarly, the high degree of openness of architecture and the ability to customize the solution on part of the end-user were also common traits for the various solutions. The idea that clients want to adapt the solutions

to their specific needs, which often change across time, is commonly accepted in the industry. Most firms have indicated that they either offer their users the ability to adapt the solution as they like, or offer them their services to do so on part of the clients. This flexibility is probably something we take for granted today, but it has not traditionally been a trait for such solutions.

Moreover, the ability to offer advanced analytics and machine learning as a means of coping with the fast-rising transaction volumes and stringent regulatory requirements is another important feature of the more sophisticated solutions. This technology also helps firms to get control of the false positives and false negatives that can be generated when dealing with a high number of transactions.

Similarly, another upcoming aspect is the use of alert of alerts to obtain valuable information from specific groupings of alerts and the use of machine learning to improve the system's ability to detect instances of money laundering over time. It is not sufficient to just have advanced technology for detection, however, it is important to have configurable dashboards that are user friendly and help the clients achieve their goals in a time-effective manner. Many vendors have tried to achieve this and have, by and large, met with success in their efforts to do so.

Kapronasia is a leading provider of market research covering banking, payments, capital markets, and insurance. From our offices in Shanghai, Hong Kong, New Delhi, and Singapore, we provide clients across the region the insight they need to understand and take advantage of their highest-value opportunities in Asia and help them to achieve and sustain a competitive advantage in the market.

For more information about Kapronasia, please email:  
research@kapronasia.com or  
visit <http://www.kapronasia.com>

**kapron**  
**ASIA**