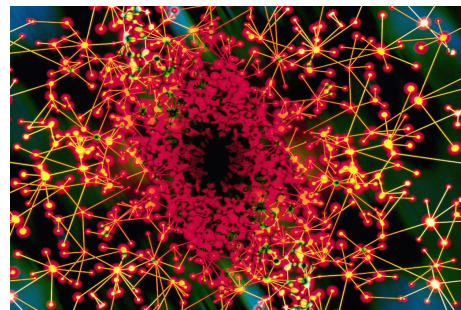


Implementing AML Transaction Monitoring Software

Even the best technology will not completely stop all money laundering or terrorist financing activities. However, adopting software to monitor transactions demonstrates a financial institution's commitment to be a good corporate citizen, a willingness to improve governance and best practices, and a concern for customers, says Dominic Nixon, Asia Head for AML, PricewaterhouseCoopers.



Dominic Nixon and *Rohan Bedi*, Head of AML Services, PricewaterhouseCoopers Singapore, talked to Michael Thomas, Group CEO of STB Systems UK which develops anti-money laundering software, to find out how their product works, how it is implemented, who manages the system and what new features are being developed to cope with changing demand.

What does anti-money laundering (AML) transaction monitoring software (TMS) supposed to do?

Rohan: It supports the due diligence process when a customer wants to open an account. This requires verification of the identity and address details and source of funds of a prospective customer. From a technology perspective, it is quite a simple approach to ensure that the required documents are present (if electronic document storage is implemented) and to verify that the account due diligence process has been performed. TMS can conduct auto-check transactions in real time. Some packages can perform hot-list checks and even stop transactions in real time. The US Office of Financial Assets Control Check alone is against a hot-list of more than 5,000 items. Software can also be used to do transaction profiling, where account and customer level,

checks are made against transactions of that customer and his/her peers. Auto-alerts can be generated on a priority basis, with alert and background details (for example, alert triggers, access to transaction data and previous alerts, and related accounts), providing an automated workflow to the relevant person. Most TMS systems are capable, in varying degrees, of incorporating new information or performing additional interrogations based on new ways of recognising suspicious transactions. Many applications can track the clearance of flagged transactions and automatically highlight required outstanding action-items or issues and generate e-mail reminders. This is a critical feature for money laundering reporting officers. Suspicious transaction reports (STRs) can be automatically generated inclusive of all key customer information for reporting purposes. Complete audit trails are automatically maintained for regulators' inspections. Typically, the audit trail captures details regarding opened, cleared, closed cases, any STRs generated, and so on. Management and compliance reports provide aggregated information and statistics that highlight high-risk customers and the overall efficiency of the "know your customer" process - a critical feature for monitoring your overall risk exposure and identifying training needs.

Take us through the key features of a TMS package, for example, STB-Detector? What does it consist of? How does it work?

Michael: We have built a modular system with four parts:

- First, we have the Account Opening and Due Diligence module, which helps institutions ensure that they have the right documentation to support the type of business a customer is transacting with them. We localise this to refer to the types of proof of identity that are available in the locale, for instance some countries have ID cards for all nationals and others do not, some of these contain photos and again, others do not. Electronic copies of the documents held can be linked to the customer details and the system will automatically check, if the customer starts to transact a new type of business, that the documentation held will support that business and it will also remind you when a piece of documentation needs to be renewed, such as when a passport is about to expire.
- The second module, Suspicious Activity Monitoring, performs the type of statistical analysis and profiling that cannot be achieved manually. Again, some of the validations it performs are localised, such as specific cash limits set in the different jurisdictions that are automatically reportable to the authorities. We also implement checks just below the local requirements to pick up anyone deliberately avoiding a published limit. The system performs historical analysis of business transacted by the customer, by peer groups and within the type of business. It then looks for any unusual activity through a statistical analysis of what it finds, putting the exceptions onto the compliance managers desktop,

where they can readily manage the workflow of all exceptions. It is then for the compliance manager to investigate further and decide whether the activity is genuinely suspicious, and therefore reportable, or not.

- Third, we have the Watch List Monitor, which checks transfer parties (originator, beneficiary and the narrative fields) and the existing customer database for any listed undesirable individuals and corporations that people shouldn't be doing business with. Any number of lists can be combined, the MAS list, OFAC, United Nations lists, Politically Exposed Persons lists, an institutions own lists etc. for checking purposes.
- Finally, we have an Investigations module, which will search for given names throughout the history of payment stored within the system. This is very useful when the authorities are conducting criminal investigations and want an institution to report everything they have processed for someone in, say, the last two or more years. Our system retains the payments data daily to facilitate this, which is something that the real-time filters don't keep.

What key steps need to be taken during the implementation process?

Michael: There are a number of steps an institution needs to go through:

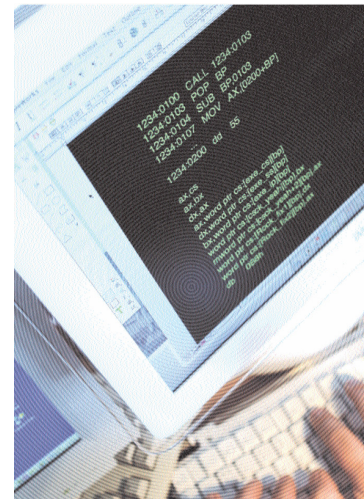
- The very first stage is an overall risk assessment, which ideally should be conducted independently of potential suppliers of parts of what might be required in a final solution to managing money laundering risk. The business needs to know what risks it is running given the type of business it is transacting and the legal and regulatory framework in which it operates. It is for senior management to agree upon their appetite for risk. They are then in a position to start thinking about how to reduce or eliminate some of those risks, and automation will only be one part of what should be an integrated approach to money laundering risk management.
- We then commence the IT project by analysing the data environment the institution has to see where the data we will need is to be sourced from and identify any potential issues of data consolidation. If data resides in any standard database that complies with the Open DataBase Connectivity standards, such as Oracle, Sybase, SOL Server etc, we can directly register to the data tables to access the data we need. With legacy systems a data download will be required.
- The writing of these business rules is the next stage in the process. This is not a highly technical issue. We use business people to write the rules, not programmers, which means the resultant configuration is transparent to the end user.
- It is then a matter of configuring the reports relevant to the business, possibly developing some additional ones to the customer's specification, which is again made easy using our own report writer. We then feed the data through and adjust tolerances and thresholds, being

mindful of the risk framework defined by the institution at the outset. Ideally the customer can provide a certain amount of historic data so that the tolerances can be tuned early on, otherwise the user will have to make adjustments as data history is accumulated every day after implementation and the system begins to understand what usual activity is.

- Finally the users are trained to manage the system end-to-end, from data acquisition through to the compliance manager's desktop, but training only usually takes one or two days. Depending on the complexity of the institution's IT infrastructure the project could take several months or just weeks if we are dealing with a single source.

Who normally manages the system once it goes live?

Michael: Responsibility for managing the system normally rests with the compliance manager or the compliance team in larger organisations. IT may be involved in running the overnight processes to deliver the data, normalise it, answer queries and report any exceptions to the compliance manager's desktop, but all of this processing can be automated as well, thus bringing ongoing IT involvement down to simple maintenance of any bespoke downloads should the data requirements or source systems change. Of course, it is not uncommon for source systems to change over time. The tolerances, thresholds and business rules that perform the queries are normally managed directly by compliance people.



In some instances, our customers use the system for wider reporting of exceptions or combine it with some of our other products. In these cases different users are able to access a different set of functions and receive their own individual set of reports. Everything in the system is controlled from the users sign-on, so they can only access what they are authorised to run and what they are authorised to see. It is essential that compliance applications of this importance have strict security built into them so that they can never be compromised.

Is the system fully developed, or are you still adding new functionality?

Michael: The system is fully developed and running live at client sites, although in some ways I think an AML solution can never be fully developed. We have to respond to any newly identified typologies and introduce the business rules to trap them, so we will always be

providing our customers with small enhancements to strengthen their defences. In addition we are looking at establishing relationships with some of the data suppliers, companies that provide managed lists of the names of prohibited persons and corporations, politically exposed persons, and linking in their data. Specifically, we are looking at enhancing our product with a Link Analysis technology, although this will be most useful at the upper end of the market.

Can your product deal with the new FATF requirements relating to funds transfers?

Michael: FATF special recommendation seven on anti-terrorist financing urges countries to take measures requiring financial institutions to include accurate and meaningful originator information about fund transfers and related messages that are transmitted (domestic/cross-border), and that the information should remain with the transfer or related message throughout the payment chain. Certainly - the STB-Detector software can assist banks to deal with their new due diligence requirements related to heightened information availability and also the recommendation to retain data for five years.

So how do you go about identifying the different typologies and implementing defences against them?

Michael: Many of the financial regulators now issue potential typologies and details of specific cases they have encountered. In addition, the Financial Action Task Force and other national and international bodies issue regular case studies and provide advice to institutions. We keep in touch with these and monitor for new methods. We also have the advantage of operating around the globe so we pick up on the views of many regulators and also get plenty of feedback from the demonstrations we perform and from working with new clients. Everything gets fed back to our head office and, if we find something that we do not currently have an adequate check against, we simply define a business rule search to highlight the new suspicious activity.

What in your opinion are the types of activity that particularly affect the Asia-Pacific region?

Michael: Yes, there are some types of activity that are more prevalent in Asia-Pacific, although most also apply elsewhere. For instance, the removal of the Taliban regime has resulted in increased drug production in Afghanistan so, there needs to be more vigilance over funds that terminate in South Asia. The consumption of synthetic drugs in Southeast Asia is on the rise - hence the proceeds of drug sales will need to be laundered. Illegal gambling is a significant

issue in Hong Kong just as prostitution is in Thailand, and, quite clearly, terrorist funds are being moved within the area, especially with the clamp-down in the Middle East, with the horrific result being the Bali bombing, and of course cash remains an important means of settling transactions in the region, which makes it more difficult to spot criminal funds being mixed in with legitimate money. Cross border smuggling of cash and bearer instruments is an issue just as underground banking operations is also a critical issue. That is why institutions must monitor for changes in the pattern of business across an account, which could indicate funding being provided for an imminent terrorist event or money laundering. They must look for significant payments moving across borders, particularly certain countries known to be the source or a key conduit for drugs, both harvested and manufactured. They need to be able to define peer groups of customers in order to be able to detect an exceptionally high amount of cash deposits by one or two members of the peer group. Systems can identify all of these scenarios, but then it comes down to the institution's compliance staff to look more closely and to report truly suspicious events to the authorities for them to investigate. We provide the local forms within the system and in some cases link directly to the police or other governing authorities to report them, but only after the user has declared that an exception found by the system is a reportable event.

What in your opinion are other activities that institutions should be wary of?

Michael: It is important that institutions consider other ways that criminals move money, so they should look at payments being made to gold or precious gems companies, as this could indicate the conversion of criminal money into a physical medium that is easy to transport and re-convert into cleaned funds in a different geographic location. It is vital that institutions correctly code businesses in their systems so that these types of transaction can be readily tracked.

Transparency Internationals Corruption Perception Index 2002 also points to high levels of perceived corruption amongst many Asian governments. This exposes Financial Institutions, especially Private Banks, to the risks of Politically Exposed Persons.

Also, institutions need to be aware of the threat of internal fraud or collusion. There was a recent case in Singapore of employee's withdrawing relatively small amounts from accounts of deceased customers. Because the amounts were small no one noticed. However, a detection system would have highlighted these withdrawals, as even a small withdrawal from an account that has been inactive for a considerable time would be statistically significant. Whilst the occasional account will behave this way, clearly in this particular instance a pattern would soon

have been noticed and the perpetrators could have been intercepted sooner.

As I said earlier, we do our best to monitor for different typologies so that we can continue to maintain the highest degree of protection within our solution, but it is also the responsibility of the institution to contribute to this process and proactively manage their implementations, particularly when managing internal risks of fraud which are affected by the internal business structure. Our solution is open, flexible and easy to tune in this way.

Is there a multi-lingual version of the system?

Michael: We have designed the product so that it could be delivered in languages other than English, although it has never been a requirement thus far. Some of our regulatory reporting products already show regulators forms in Chinese and Thai, for instance, and we can readily handle data held in these character sets, but no-one has requested the system itself to be translated. As regards AML, there is a problem with using non-English languages because all of the international watch lists are issued in English, although some national lists are issued in different languages. I am sure that criminals and terrorists are aware of this and exploit countries that operate their IT systems in different languages knowing that their English names on say the OFAC list cannot be directly translated into say Chinese.

Reprinted from Banking Today, the Journal of the Hong Kong Institute of Bankers, May/June 2003, By Joanne Lee-Young