Compliance Digest

ISSUE 06 | March| 2018

AFRASIA bank different

Dear Readers,

Welcome to the 6th issue of our Compliance Digest which brings to you compliance and risk management related articles.

This issue gives you the necessary updates in the Guidelines, Rules and some recent Supreme Court Judgements.

Readers will also benefit from articles such as The many challenges of mobile computing, An introduction to the 360 degree AML investigation model, Keeping pace in the age of sanctions and Holistic trade surveillance amongst others.

Finally, you will browse some Compliance news around the world.

We wish you a pleasant reading!

Anil Fangoo, CAMS
Group Head Compliance & Editorial Team

Evolving Compliance - Is your program adaptive?

Building a compliance culture requires teaching people, at every level, how effective choices are made. People learn ten percent of what they read, thirty percent of what they see, fifty percent of what they hear and see, seventy percent of what they say or write and ninety percent of what they do. So why are most organisations providing employees learning tools that only get them to about fifty percent efficacy when the stakes are so high?

Most of us are not aware that technology can now achieve the most fundamental tenet of how humans are wired to learn: a learn-by-doing experience tailored to who you are and what you know. This is called adaptive learning.

Adaptive learning allows employees to be the masters of their own destinies, reducing fatigue and frustration while minimising the loss of productive time and delivering better educational outcomes.

Implementing an Adaptive Learning Approach

To decide whether adaptive learning could improve your compliance program, ask yourself these five basic questions about the learning tools offered within your organisation: (i) Are they teaching people to "do" instead of "read and see"; (ii) Are they optimising seat time and personalising learning paths for every employee?; (iii) Are they generating indicative data about employee choices that impact the organisation?; (iv) Can I measure effectiveness and benchmark performance internally and against industry peers? And (v) Are they arming me with a clear way to prove that each learner obtains proficiency?

Source: Corporate Compliance Insight

IN THIS ISSUE

Follow Us on

COMPLIANCE & EDITORIAL TEAM

Anil Fangoo | Raveena Doolhur | Khusboo Puryag | Vashish Bundhun | Daniella Bungaroo - Pothiah | Adeline Li | Deshen Narayanan | Sonya Mohadeb

RECENT ACTS, REGULATIONS, RULES & GUIDELINES

Bank of Mauritius Guidelines	Effective Date/ Amendment Date
Guideline on Credit Risk Management (Amendment)	August 2017
Guideline on Credit Concentration Risk (Amendment)	September 2017
Guideline on Corporate Governance (Amendment)	October 2017
Guideline on Liquidity Risk Management (Amendment)	October 2017
Guideline on Outsourcing by Financial Institutions (Amendment)	November 2017
Guideline on Credit Concentration Risk (Amendment)	December 2017
Guideline on Maintenance of Accounting and other records and Internal Control (Amendment)	December 2017
Acts	
Data Protection Act 2017	January 2018
FSC Act/Rules/Regulations	
Financial Services Act 2007(Amendment)	July 2017
Securities Act 2005 (Amendment)	July 2017

Source: BOM and FSC websites

Summary of Guideline on Outsourcing by Financial Institutions

The main amendments are the additions of two new sections on Cloud – based Services and Annual Reporting:

Cloud – based Services

Bank of Mauritius:

(i) considers cloud-based services operated by service providers as a form of outsourcing and recognises that financial institutions may have recourse to such services to enhance their operations and service efficiency.

(ii) expects financial institutions to be fully aware of cloud-based services characteristics such as multi-tenancy, data commingling and the possibility for processing to be carried out in different locations.

Cloud-based services are subject to the same types of risks as in other forms of outsourcing arrangements.

Financial Institutions:

The usage of cloudbased services shall be restricted to non-core activities only.

- to perform the necessary due diligence and apply sound governance and risk management practices when subscribing to cloud-based services.
- required to take appropriate measures with respect to data access, confidentiality, integrity, sovereignty, recoverability, regulatory compliance and auditing.
- ensure that the service providers have the capacity to identify and segregate customer data using strong physical or logical controls.
- ultimately responsible and accountable for maintaining oversight of cloud-based services and managing the attendant risks of adopting cloud-based services, as in any other form of outsourcing arrangement.

The implementation of cloud-based services by financial institutions would be subject to conditions.

Annual Reporting

On a yearly basis, a list of all material and non-material activities that have been outsourced is to be submitted to Bank of Mauritius, in the form and manner prescribed.

This list should be submitted within the next twenty working days of the previous calendar year.

SUMMARY OF THE DATA PROTECTION ACT 2017

The objective of the Act is to repeal the Data Protection Act 2004 and replace it by a new and more appropriate legislation.

The Act aims:

- to simplify the regulatory environment for business in the digital economy and promote the safe transfer of personal data to and from foreign jurisdictions; and
- to be in line in particular with the European Union's General Data Protection Regulation 2016/679 ('GDPR) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
- The inclusion of new definitions, such as biometric data, blocking, data matching, genetic data, personal data breach, profiling, and pseudonymisation, as well as the expansion of the definition of consent, demonstrate the efforts of the legislators to bring the Mauritian data protection framework into line with the EU's.
- This is further highlighted by the addition of provisions regarding current issues, including the threshold for child's consent, which, as in the GDPR, the Act sets at 16 years of age.

Privacy Impact Assessment

If an organisation implements technologies which could result in high risks to the rights and freedoms of data subjects, a privacy impact assessments (PIA) must be carried out.

Consent

- Consent must be freely given, specific, informed and unambiguous - this can be done by a statement or a clear affirmative action.
- The data controller is required to demonstrate that consent has been given.

Data breach notification

- The Act makes personal data breach notification mandatory.
- A personal data breach must, without undue delay and, where feasible, not later than 72 hours after [the data controller] has become aware of the breach, be notified to the Data Protection Commissioner.
- If the data breach is likely to result in a high risk to the rights and freedoms of data subjects, the data controller must notify them of the breach. As provided under the GDPR, there are exceptions to this obligation.

Data protection officer

- Both data controllers and data processors are now required to appoint a data protection officer.
- With the onerous obligations which are imposed on data controllers and data processors, data protection officers will need to be well conversant with the provisions of the data protection legal regime.

Accountability

- Accountability obligations are imposed on data controllers. These include requiring them to conduct an assessment of the impact of high risk processing operations, and to keep records of processing operations.

The Data Protection Office will encourage compliance with the new law by laying standards for certification mechanisms, seals and marks. Like under the GDPR, certification is voluntary.

However, there are differences between the Act and the GDPR. The large administrative penalties included in the GDPR have not been incorporated into the Act. Rather, the Act proposes, on conviction of a criminal offence, maximum fines of MUR 200,000 and prison sentences of up to five years.

RECENT SUPREME COURT JUDGEMENTS

JAULIM PLAZA LTD v. BRAMER BANKING CORPORATION LTD & ANOR [2017 SCJ 368]	The plaintiff was the holder of an account with Bramer Banking Corporation (**Bank**). On 3 April 2015, the co-defendant (**BOM**) revoked the licence of the Bank and appointed Messrs André Bonieux and Mushtaq Oosman as Receiver Managers for the Bank. The plaintiff alleged that Mrs. Bilkiss Banon Jaulim transferred an amount of Rs 4,300,000 to the plaintiff's account. After confirmation of the transfer, the plaintiff made several payments from the said account. On 10 April 2015, the Bank debited the plaintiff's account by an amount of Rs 4,300,000 without its consent. The Court referred to the authoritative pronouncement made by the Judicial Committee of the Privy Council recently in the case of **Mediterranean Shipping Company v. Sotramon Limited [2015 PRV 105]** which was applied to the present case. The Judicial Committee reaffirmed the established doctrine that parties who are linked by contract must ground any claim that they may have against each other, on the basis of contractual liability and not in tort. A « *cumul de la responsabilité contractuelle et de la responsabilité délictuelle* » is not permissible under the Mauritian Code. Civil Liability could either be based in contract or in tort and the basis of liability is an exclusive one. The debiting of any sum of money from the plaintiff's account without his consent, approval or authorisation tantamounts to a breach of the contractual obligations which govern the bank/client contractual relationship which admittedly existed between the parties. It was therefore not in order for the plaintiff to proceed with the claim for *faute* grounded in tort with respect to what clearly tantamounts to a breach of the contractual relationship between the Bank and its client. Any action against the Bank in the light of the averred facts could only be based on "*faute contractuelle*" and not "*faute délictuelle*". In view of the above, the Court found that the plaintiff's claim was fundamentally flawed and non-suited the plaintiff.
BARCLAYS BANK MAURITIUS LIMITED v KARAMUTH O & ORS [2017 SCJ 313]	On 21 February 2012, an interim order in the nature of a Mareva injunction was issued prohibiting all the respondents from disposing their movable and immovable properties, including bank accounts, and from removing from Mauritius any of such properties or assets. The applicant bank prayed that the interim order is made interlocutory. With regard to principles governing Mareva injunctions, the following extracts from Steven Gee, Mareva Injunctions and Anton Piller Relief, Fourth Edition, were referred to:- "*The purpose of Mareva relief before judgment is to prevent unjustifiable dissipations or dealings with assets which are liable to result in a judgment of being unsatisfied…. the relief is not to be granted except when the court is satisfied that:-* *the plaintiff has a good arguable case against the defendant; there is a real risk that judgement will go unsatisfied by reason of the disposal by the defendant of his assets, unless he is restrained by court order from disposing them; and it would be just and convenient in all the circumstances of the case to grant the relief sought…..* *In Mareva cases the all-important question is whether, in the circumstances of the case, it is 'just and convenient' to grant the injunction.*" Evidence on record revealed that a fraud of some Rs.50 million was perpetrated to the prejudice of the applicant. The Court ordered that the Mareva injunction issued against all the respondents on 21 February 2012 be made interlocutory pending the disposal of the main case which had already been lodged.

RECENT SUPREME COURT JUDGEMENTS (CONTINUES)

ROUILLARD E. & ANOR v THE MAURITIUS COMMERCIAL BANK LTD [2017 SCJ 380]	The case involved an application to set aside a bankruptcy notice served by the respondent on the applicants. The respondent raised a preliminary objection to the effect that there remained an amount outstanding on the judgement debt. The applicants, on the other hand, contended that they had settled the whole debt, no outstanding amount remained and that they had in fact paid in excess of the amount due. There was no specific provision as per the law for the setting aside of a bankruptcy notice. However, under the Insolvency Act, section 8(2)(a) lists out as one of the requirements of the bankruptcy notice that the "*creditor has obtained a final judgment or a final order against the debtor for any amount*". Another alternative requirement is to be found at Section 8(3)(a), that is "the debtor is indebted to the creditor in relation to a 'provable debt' ". In its judgement, the appellate court ordered the applicants to pay to the respondent "*jointly and in solido the sum of Rs 3.5million with interest*", without particularising the precise amount due as interests. As such, each party has carried out its own calculation of the interests due and had reached different figures. It was not disputed that an amount of Rs 3.5M together with an amount of Rs 54,587 being interests at the legal rate of 8% as from the date of the judgment of the appellate court until the date of payment, as well as half costs in the sum of Rs 16,300 was paid. The amount claimed by the respondent was not therefore an amount which had been quantified with finality, so that it was highly questionable whether a "*final judgment*" existed or a "*final order*" as contemplated by Section 8(2)(a). The application was accordingly granted and the bankruptcy notice was set aside.
MAUDARBOCUS S M E N v THE MAURITIUS COMMERCIAL BANK LTD [2017 SCJ 388]	The applicant had sought before the Judge in Chambers an order prohibiting and restraining the respondent from disposing an immovable property pending the determination of a main case. The application was set aside. On appeal, the Supreme Court upheld the decision of the Judge in Chambers. The applicant was now applying for leave to appeal to the Judicial Committee of the Privy Council against the decision of the Supreme Court. Section 81 of the Constitution entitles a party to civil proceedings to appeal as of right only against a "*final decision*" of the Court of Appeal or the Supreme Court and that a "*final decision*" within the meaning of that section is one which finally disposes of the matter in litigation or the rights of the parties. The Court referred to the case of *Ramlagun v Indian Ocean International Bank Ltd [1990 MR 229]*, where the Judge in Chambers refused an application for an interlocutory injunction to restrain the respondent from disposing of an immovable property on the basis that an interlocutory injunction was merely provisional in nature and did not conclude a right. It held that a final decision was one which finally disposed of the matter in litigation and must be distinguished from an interlocutory one. It was held that the decision of the Supreme Court upholding the judgment of the Judge in Chambers did not finally dispose of the matter in litigation or practically put an end to the litigation. It was, therefore, not a "*final decision*" against which an appeal lies as of right under section 81(1)(b) of the Constitution. Leave to appeal was refused.

Source: Supreme Court Website

RECENT SUPREME COURT JUDGEMENTS (CONTINUES)

BLACK RIVER TRUST COMPANY LTD v THE FINANCIAL INTELLIGENCE UNIT & ORS [2017 SCJ 420]	The case involves an investigation by the UK authorities into offences of cheating the public revenue, fraud, false accounting and money laundering having been allegedly committed by certain British nationals. Disguised payments were allegedly made to individuals and other companies, which were not accounted for, to the HMRC. A Restriction Order was issued at the request of the respondent to prevent the persons who are subjected to criminal investigation in the UK from disposing of the sums held in bank accounts in Mauritius. In pursuance to sections 29 and 31 of the Asset Recovery Act, the applicant was praying for a variation in the Restriction Order to remove certain bank accounts held with the Co-Respondents from the purview of the said Order. The Asset Recovery Act 2011 makes clear distinction of the circumstances in which a Restraining Order and a Restriction Order would be issued. For a Restraining Order to be issued, the Judge must be satisfied, firstly, that a person has been charged with or convicted of an offence or a criminal investigation is on-going. Secondly, there is reasonable ground to believe that the property, the subject of the application, is proceeds of an offence. On the other hand, for a Restriction Order to be issued, the Enforcement Authority has only to show that the property is reasonably believed to be "*proceeds*" "*without having to show that the property was derived directly or indirectly from a particular offence or that any person has been charged in relation to such an offence*." In its second affidavit, the applicant had taken a preliminary objection that: "*ex-facie the application for the Restriction Order dated 28 March 2017, the respondent acted ultra vires its powers and it had no locus standi to lodge the said application. The applicant therefore moves that the Restriction Order made on 28 March 2017 be purely and simply rescinded having been improperly lodged by an entity which had no locus standi to do so*." The Court held that the respondent was fully entitled to apply for a Restriction Order for properties reasonably believed to be "*proceeds*" without having to show that the property was derived directly or indirectly from a particular offence. In line with section 5 of the Mutual Assistance in Criminal and Related Matters Act 2003, the respondent had the locus standi to apply for an ex parte application and the Restriction Order was lawfully issued. The preliminary objection was therefore ill founded and was accordingly set aside. With respect to the bank accounts held with Investec Bank, the respondent was not disputing the fact that three certain bank account numbers were included in the application for the Restriction Oder through oversight. The Court accordingly varied the Restriction Order and excluded those account numbers from the Order. With regard to the bank accounts held with SBM Bank and AfrAsia Bank, the Court was not satisfied that the applicant had discharged the burden of showing that those bank accounts were not subject to investigation by the UK authorities. The Court therefore made no order for a variation in respect of the accounts held with SBM Bank and AfrAsia Bank.

Source: Supreme Court Website

THE VARIOUS COMPLIANCE CHALLENGES OF MOBILE COMPUTING

Mobile computing has become increasingly significant due to the rapid rise in the number of portable computers and the desire to continuously have network connectivity. Mobile computing, also known as "human-computer interaction", is a generic term used for a variety of devices which allows individuals to access data and information from wherever they are and involves the transportation of data, voice, and video over a network through the devices.

Some of the most common forms of mobile computing devices are portable computers, mobile phones, smart cards that can run multiple applications but typically payment, travel and secure area access, wearable computers etc.

While mobile computing encompasses challenges, it also presents unique difficulties to compliance officers in banking. Professionals/bankers are increasingly expected to use their own devices for work that is, connecting to corporate networks and systems through virtual private networks (VPN) from home desktops and laptops to loading work email accounts on personal smartphones. Most individuals only worry about loss of devices when in fact important corporate data can reside or pass through their mobile devices. It is therefore imperative to ensure professionals act in compliance with the laws and regulations of data protection so that confidential information is not at risk of divulgence.

Network security in mobile computing should be of greatest concern. While most public Wi-Fi hotspots are unencrypted, anyone within range can collate data which is sent or received, for example, emails with attachments containing client data. Also at risk are temporary and cached files on mobile devices since they contain data that should be protected, such as through VPN channels, network addresses and log-in information.

The reality is such that data on the device should be the priority. The owners of mobile devices, whether personal or corporate should not underestimate the significance of basic security features such as password protection, two-factor authentication, encryption and the ability to wipe/lock devices remotely if same are lost. As a precautionary measure, confidential information/client data should not be directly/indirectly exposed while in a public area.

In addition to the above-mentioned measures, trusting that professionals who are working in the right culture do the right thing when given the right information must be the preferred model.

Source:https://www.thebalance.com/definition-of-mobile-computing-2533640
http://www.corporatecomplianceinsights.com/many-compliance-challenges-mobile-computing/
https://ijact.in/index.php/ijact/article/viewFile/256/208

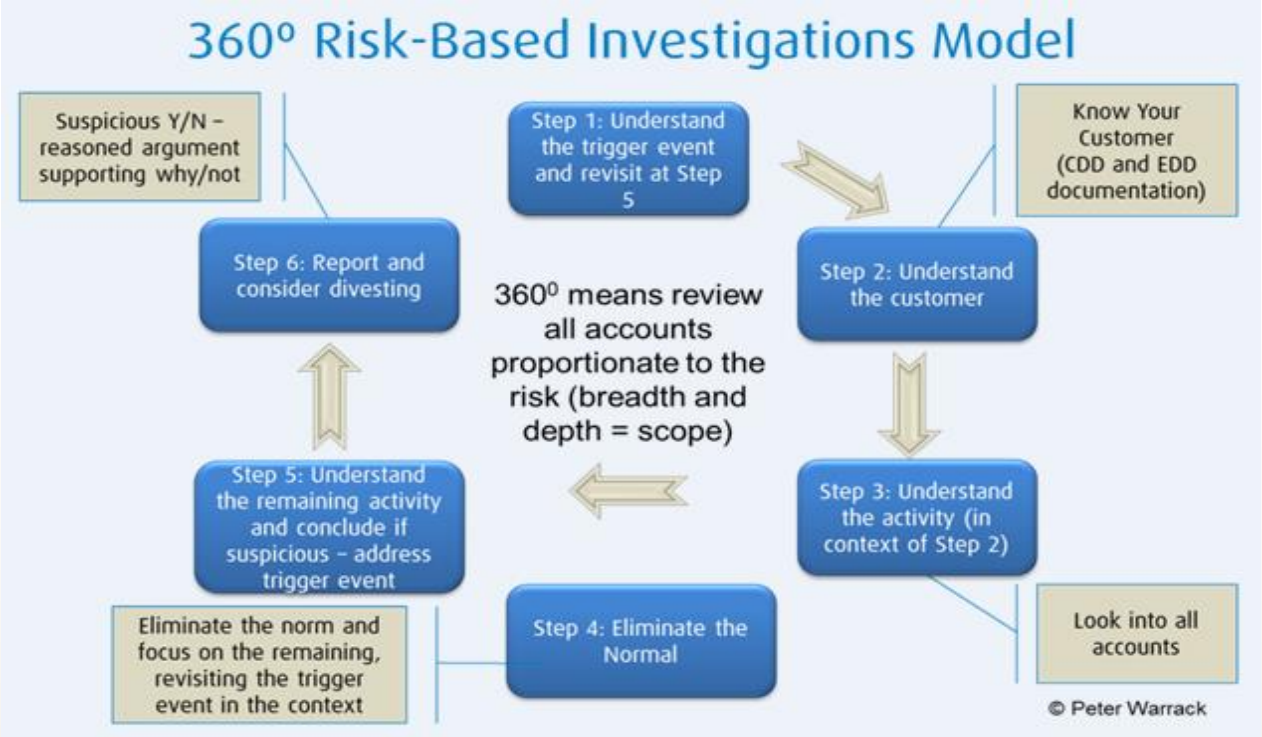
AN INTRODUCTION TO THE 360 DEGREE AML INVESTIGATION MODEL

AML/CFT investigation models historically relied on qualitative and expert judgment components. However, while these models still currently rely on expert judgment, they are coupled with more sophisticated scoring algorithms and have other quantitatively derived components, such as thresholds of transactions, risk based assessment and type/segments of customers and transactions.

To better identify suspicious transactions and conduct an investigation the AML Thinking Map may be used. It is a tool designed in prompting thought to ensure an investigator so as to ensure that all relevant bases are covered the relevant questions are asked. The thinking map provides consistency and robustness to investigations and ensures that important parts are covered. Furthermore it changes the way investigations are conducted and involves a change in mindset. This means that a systematic risk-based methodology should be used instead of a tick-boxing approach . At the same time it encourages banks to empower and train relevant staff to think and take a decision when monitoring the transactions.

A template of the AML Thinking Map is as per below table:

Customer Identity and Verification	**Customer Occupation or Business Activity**
♦ Do we know who the customer is, as opposed to who they purport to be? ♦ How long has the customer relationship been established? ♦ How is their individual or corporate identity confirmed? ♦ Is their individual or corporate identity supported by authentic and appropriate documentation or other sources? ♦ What reliance can be placed on supporting documents or information? ♦ Does the information provided by the customer correspond with our findings? ♦ Is the customer included on any sanctions lists or negative databases? ♦ Is there relevant adverse information? ♦ Does it all make sense?	♦ What does the customer do? How do they earn their living? ♦ What is the nature of risk associated with their declared occupation? ♦ Is the occupation or activity legitimate and/or within bank policy? ♦ How is the customer's occupation verified? ♦ Is the customer's income consistent with their occupation? ♦ What evidence exists to support the income? ♦ What reliance can be placed on this evidence and how can it be tested and confirmed? ♦ Does the information provided by the customer correspond with our findings? ♦ Does it all make sense?
Source of Funds	**Destination of Funds**
♦ What is the source of funds under review? ♦ What is the source of funds used to open the account? ♦ What evidence exists to support these sources of funds? ♦ How much reliance can be placed on this evidence and how can it be further confirmed? ♦ Is the source legitimate and consistent with the customer profile? (Consider evidence of predicate offenses). ♦ Is the source in itself high risk (i.e., by the industry or country?) ♦ Are there any associated sanctions risks? ♦ Is the source within bank policy? ♦ Is the customer entitled to these funds? ♦ Does it all make sense?	♦ What is the destination of funds transacted? ♦ Who is the beneficiary? ♦ Who is the ultimate beneficiary? Do we know? ♦ What evidence exists to support the above? ♦ How much reliance can be placed on this evidence? How can it be further confirmed? ♦ Is the destination in itself high risk (i.e., by the industry or country)? Are there any associated sanctions risks? ♦ Is the destination within bank policy? ♦ Is the beneficiary entitled to these funds? ♦ Does it all make sense?
Product and Transaction Type (Types of Funds)	
♦ Is the type of product consistent with the customer's profile? ♦ Why is the customer using this product (i.e., drafts and not wires etc.)? ♦ What is the risk associated with the product? ♦ Nature of the transactions (volume, amounts, locations, use of other financial mediums, etc.) ♦ Are the transactions consistent with the customer profile and declared activity? ♦ Does it all make sense?	



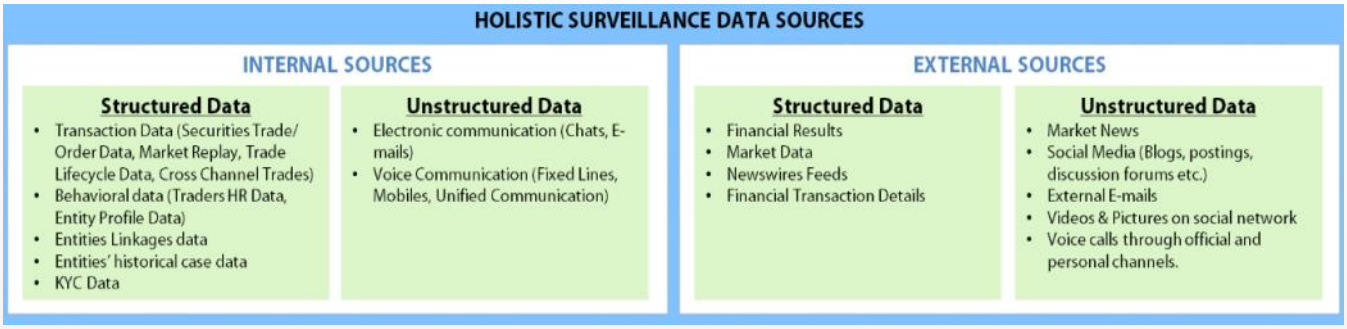
The six step 360 Degree Risk-Based Investigations Model provides consistency of approach and applies critical thinking thought processes to determine if the transaction or proposed transactions are suspicious or not. Using an all-inclusive approach, this model reviews all customers activity and profile, taking into consideration both the extent of other connected customer relationships and the previous transactions. Details of the steps to follow are as per below:

DETAILS OF STEPS
Step 1: Trigger – The investigation is prompted through either a transaction monitoring alert, adverse information on the press/internet or a suspicious transaction report. It is vital for the investigator to understand the trigger, which provides the initial key information concerning the issue and investigation to be done.
Step 2: Understand the Customer - Know Your Customer is the most vital part AML/CFT investigation and must be done on an ongoing basis. KYC documents and Customer Due Diligence information as per KYC records of customers, which must be held at the bank. The bank must understand the type of customer, their profile/activity/profession, source of wealth/fund, the banking/financial products and services they are using, jurisdiction/country of residence/ incorporation/exposure/operation, link to sanctioned parties/countries, parties linked to the customer, adverse information on press/internet and other independent searches.
Step 3: Understand the Activity – This allows the investigator to understand if all the transactions for the review period matches the profile/activity of the customer.
Step 4: Eliminate the Norm – Activities which are in line with the profile/activity of the customer may be considered as being not suspicious and thus only some specific transactions/activities may be highlighted for further investigations. Normal activities may include personal expenses, rent and transport for Individual customers and invoice payments, payroll, IT & Marketing payments and salary payments for Corporate customers.
Step 5: Understanding the Remaining Activity to conclude if it is suspicious or not – Once the normal transactions which matches the profile/activity of the customer are eliminated, the other transactions must be further investigated. Many factors must be taken into consideration and the specific transactions must be reviewed and analysed along with the trigger event and KYC documents/CDD information held by the bank. Furthermore the assessment of suspicion must be based on a reasonable evaluation of relevant factors, including the knowledge of the customer's business, financial history, background, and behaviour. Based on his knowledge and experience and known indicators of money laundering and/or terrorist financing, the investigator must therefore conclude if there are reasonable grounds to suspect that a transaction is related to the offences of Money Laundering and/or Terrorist Financing.
Step 6: Report & Document – If required, a Suspicious Transaction Report must be submitted to the relevant authority, in a timely manner. Furthermore, the full investigation must be properly documented.

Source: http://www.acamstoday.org/introduction-360-degree-aml-investigation-model/

HOLISTIC TRADE SURVEILLANCE - A NEW PARADIGM IN SECURITIES MARKET COMPLIANCE

In today's global economy, it is important to have an effective regulatory compliance that encompasses cross-asset class and cross-market trade surveillance, monitoring activities for market manipulation, fraud, behavioral patterning and more. This is what holistic surveillance is all about – it is an approach to trade surveillance which involves the consumption, monitoring and analysis of structured data and unstructured data, and draws meaningful insights/inferences using analytics-based tools that would not have been visible in isolation. Analysis of data elements include (i) trading data and pattern of participating entities (client, trader, broker, etc.); (ii) trade-related communication amongst entities; (iii) information disseminated in the market during the period in question; (iv) social media information that can be linked with the trading behavior; and (v) Human Resources and behavioral data of traders and employees of the organization.



However, holistic surveillance have certain key challenges:

- At first, isolated relevant communication information does not appear to be linked with the trade violation. In order to trace an insider, one has to scan a large volume of telephonic conversations, chat/ emails texts, etc. but may still not find any clue;
- A large number of false positive communication alerts dilute the effectiveness of communication data in providing insights to trading behaviour;
- Linking the different pieces of structured and unstructured data to create a cross-market, cross-asset class and cross-communication channel view of orders/trades depicting trading behaviour may seem to be a burdensome task;
- Decoding unstructured voice communication, which generally carries maximum information on any violation, is challenging; and
- Managing regulators' expectations with a proactive and preventive approach, as well as safeguarding against penalties.

Some potential violations in securities trading can be detected by anomalies in communication data. For example, '**Front running**' involves entering into a trade with advance knowledge of a block transaction that will influence the price of the underlying security. Orders placed just before the large block orders enter into a profit position once the block trade hits the market, indicating suspicious calls/chats were effected between the trader handling block trade and his client. Other examples are '**Insider trading**', '**Mirror trading**', '**Circular trading**' and '**Media abuse**'.

Therefore, the true power of surveillance lies in leveraging digital technologies with the relevant set of cross- channel information for creating a next generation surveillance framework. This consists of at least four surveillance 'towers', namely (a) 'A-Comms Tower' for all audio surveillance; (b) 'E-Comms Tower' for all electronic surveillance; (c) Information Security monitoring devices and the perimeter firewalls protecting from the insider threat of rogue conduct; and (d) 'HR Tower' to ensure the health and the well-being of staff by monitoring excessive working hours and/or inappropriate conversations with work colleagues. Each of these 'towers' often have separate operating teams, resulting in a highly fragmented surveillance system.

Source: ACAMS, Finextra, Nice Actimize,

KEEPING PACE IN AN AGE OF SANCTIONS

As the global geopolitical landscape grows ever more complex, keeping track of the vastly complicated web of international economic sanctions has become a daunting challenge. In order to steer clear of penalties and avoid reputational damage, compliance departments are going to have to embrace innovation.

When it comes to sanctions, it is a question that compliance professionals can relate to. As the global geopolitical landscape continues to grow more complex, there is a growing array of trade restrictions, the targets of which are in a near-constant state of flux. In just the past few weeks, alterations have been explored or enacted to sanction programs targeting entities in North Korea, China, Russia, Iran and Venezuela. The changes show no sign of letting up any time soon.

Identifying sanctioned entities and all of their issued securities, as well as detecting domestic or foreign subsidiaries (or other holdings of more than 50 percent) is a challenging task. Even trickier is deciphering the complex web of beneficial ownership rules and relationships. Corporate actions may influence the sanctioned securities, and an investment into structured products may increase the risk as well. Determining if sanctioned individuals have beneficial ownership is a critical step in putting together firms' list of "do not trade" securities that adds to the compliance challenge. On top of this, the information must be fed into the enterprise data management system, rules have to be programmed and all of the data needs to be constantly kept up-to-date.

How can financial institutions keep track of all these tasks while keeping their operation running smoothly? Those charged with protecting their firms against penalties can understandably feel like they're constantly struggling to keep pace.

Compliance departments are going to need to innovate if they want to keep up with the constant stream of new restrictions. Putting together the comprehensive, accurate and up-to-date lists of sanctioned securities needed to avoid penalties is an undertaking that challenges even the largest and most advanced organizations.

Rather than fruitlessly struggling to compile all of the necessary information by themselves, compliance departments need to innovate. New technology, or so-called RegTech, offers new possibilities for firms to automatically receive up-to-date and comprehensive daily lists of securities and entities to steer clear of in trades. These tools enable compliance staff to focus on more urgent and productive tasks, freeing traders to operate confidently and efficiently. Firms can create fully automated systems that sift through the huge quantities of necessary data, automatically alerting traders when they are in danger of violating the law and providing them with information about which sanctions a trade violates and how an instrument is attached to a sanctioned entity, saving them from the need for time-consuming research.

These innovations do not merely enable firms to keep up with the task of managing sanctions data. They make it possible for them to operate more safely and efficiently than ever before, even when sanctions regimes were relatively simple. Trades can go through without hiccups, and firms can have faith in their compliance without having to manually check each transaction. Most importantly, once compliance staffs have been freed from the constant research that sanctions once necessitated, they will be able to devote themselves to protecting their firms against more complex and serious risks.

Source: Corporate Compliance Insight

WE CAN ALL PLAY A ROLE IN FIGHTING AGAINST TERRORISM

Governments use their intelligence and law enforcement agencies to assess the level of risk or physical threat of terrorism. In this context financial institutions have to design an AML risk assessment to identify risks. Once these inherent risks have been identified, control environments must be developed to mitigate these risks. When assessing the threat of terrorism from an AML perspective, overall threat must be considered in light of terrorist financing risks. This should be assessed in conjunction with the broader terrorism risk and mitigation strategies.

The greatest immediate threat to the world comes from terrorism, which is a radical political ideology. In order to disrupt, diminish and ultimately prevent the threat of homegrown violent extremism, government must fight threat through sustainable and tactical strategies.

The tactical measures established and maintained by the government to thwart terrorist are:

- Offensive and defensive activities to include military action, diplomatic engagement, intelligence operations, law enforcement investigations and sanctioning actions.
- Initiatives to assist at-risk countries to build good governance systems and to fight corruption.
- Public and private sector financial disruption activity through disrupting the funding flows to terrorist organisations. This is where financial institutions, and more broadly the financial services industry, play a significant role. Government bodies, Public institutions and Parastatal bodies like the Police Forces, Financial Intelligence Unit, Bank of Mauritius and ICAC are organisations, which have the authority to investigate and request for information from financial institutions if they suspect any individual or entity are linked to terrorist financing and money laundering. These institutions are empowered by the law to prevent terrorist financing and money laundering. The financial institutions need to abide to the laws and regulations and must also have policies and procedures like AML guidelines and have to abide to all the authorities guidelines like BOM guidance notes, FIAMLA, POCA, POTA, Banking act 2004 and Bank of Mauritius Act 2004.
- Where required, Financial Institutions can conduct enhance due diligence on customers and have a proper due diligence process and transaction monitoring and AML software in place to track down people who are financing terrorism.
- The use of social media and internet communications to dispel and counter the appeal of radicalisation.
- Public and private sector strategies to prevent radicalisation, promote intervention and reintegration.

There are two primary Islamic terrorist residual risk factors, which are:

- Adaptability: All terrorists have demonstrated the ability to be adaptive. Just like the public and private sector assess risk, terrorists also assess counterterrorism tactics and adapt their operations to avoid detection and disruption. They also seek to continuously identify systemic vulnerabilities which they can exploit in order to sustain the threat they pose.
- Capacity and reach: Usually terrorist groups have a leader, which provides a barbaric governance. As the leader of the terrorist group collapses, sometimes another person will take over the leadership. However, in his capacity to govern may lead to rebellion in the group and can also cause terrorist attacks on innocent people.

It is difficult to eliminate the threat of terrorism. However, Financial Institutions can disrupt and prevent terrorist attacks from occurring. The financial institutions must be vigilant on an ongoing basis.

Source: ACAMS

Thomson Reuters introduces LEI profiling service to ease MIFID preparedness

In answer to a requirement taking effect on Jan. 3, 2018 that investment firms uniquely identify parties to trades or transactions under Europe's Markets in Financial Instruments Directive (MiFID II), Thomson Reuters is launching its LEI Profiling Service, a dedicated solution for financial institutions to perform a health check on their LEI (legal entity identifier) content and help them comply with MiFID II.

The forthcoming new European rules will mandate both EU and non-EU market participants (*e.g.* entities) to obtain an LEI in order to trade and clear an underlying transaction and extend it not just to direct counterparties, but also to the issuers of in-scope financial instruments.

The new service allows clients to identify those entities which have yet to request LEIs and, equally important, where LEIs exist determine their status. Upon adoption of the new service, clients send their entities of interest to Thomson Reuters, which then matches these against the LEI records stored within the Thomson Reuters Avox Database, which maintains 100 percent LEI coverage, based on daily updates from the Global Legal Entity Identifier Foundation. Since Thomson Reuters March 2017 acquisition and integration of Avox (**https://www.thomsonreuters.com/en/press-releases/2017/march/thomson-reuters-completes-clarient-and-avox-acquisitions.html**).

This growing database exceeds 2.5 million entities and covers multiple jurisdictions and entity types. The resulting unique reports returned to clients contain line-by line status on each entity record submitted.

Source: Corporate Compliance Insights: 28 September 2017

U.S, E.U Firms on bank's misconduct to top $400 billion

Regulators in the United States and Europe have imposed $342 billion in fines on banks since 2009 for misconduct, including for violation of anti-money laundering rules, and that figure is likely to top $400 billion by 2020.

Know-your-customer (KYC) and anti-money laundering (AML) processes became a key focus globally after some large global banks were hit with hefty fines in 2012, triggering a flurry of initiatives across the banking sector to boost compliance.

Major international banks are now spending between $900 million and $1.3 billion a year on financial crime compliance, according to analysis by corporate governance recruitment firm Barclay Simpson.
Source: Corporate Compliance Insights: 27 September 2017

EU introduces legislation imposing targeted sanctions against Venezuela

Following a meeting of the EU Foreign Affairs Council ("**FAC**") on November 13, it was unanimously agreed to impose restrictive measures on Venezuela. The EU has published Council Decision 2017/2074 and Council Regulation (EU) 2017/2063 (together, the "**Legislation**"). The Legislation prescribes targeted sanctions against Venezuela, including an arms embargo, with immediate effect.

The Legislation has been formulated in response to the continuing crisis in Venezuela and the perceived deterioration of democracy, the rule of law and human rights. In particular, the EU has expressed concern over the opaque and irregular election by which the Constituent Assembly was elected, and reported violations of human rights and fundamental freedoms. The EU therefore views the Legislation as a justified tool to help foster a credible and peaceful negotiated solution. The Legislation will remain in force until 14 November 2018.

Source: Global Compliance News: 18 December 2017

Angola sets up committee to oversea US$5bn sovereign wealth fund

The Finance Ministry of Angola has announced the setting up of a supervisory committee for the country's US$5bn sovereign wealth fund after an investigation revealed that its processes are transparent.

The country is also planning to increase oversight of Fundo Soberano de Angola by the ministry, the presidency and the central bank. The announcement comes days after João Lourenço, the President of Angola, sacked Jose Filomeno, son of ex-president Jose Eduardo Dos Santos, as chairman of the fund.
Source: Africa Review of Business and Technology: 18 January 2018

SUMMARY OF THE LAST ISSUE - COMPLIANCE DIGEST ISSUE NO. 5

The Compliance Digest Issue No. 5 is available via this link.

In the fifth issue of the Compliance Digest, readers were able to grasp:

- An update in the Legislations, Rules , Guidelines and recent Supreme Court Cases
- Articles on money laundering and terrorist financing risks and Vulnerabilities associated with gold, Blockain technology, Wealth management and The Russian laundromat.
- A compliance insight with Mark Andrews
- A glimpse of the global news on the financial industry around the world

Achievement of the Bank

Inauguration of AfrAsia Foundation School

AfrAsia Bank—Online Instant Bank Account Opening

Final Round from the AFrAsia Bank Mauritius Open 2017

Compliance Digest is a newsletter issued by the Compliance Department of AfrAsia Bank Limited on a quarterly basis and provides updates and important compliance and risk management issues.

The editors welcome ideas for articles in future issues. Please send your ideas or submissions to Anil Fangoo at Anil.Fangoo@afrasiabank.com or to Khusboo Puryag at Khusboo.Puryag@afrasiabank.com

AFRASIA bank different

Follow Us on