AML-CFT risk management framework evolutions

Radish Singh, Southeast Asia Anti-Money Laundering / Sanctions Leader, Deloitte Southeast Asia
Agenda

Introduction: Increased focus by regulators
Global, regional trends and developments
Impact on FCC risk management framework
Issues and expectations
Recap
Increased focus by regulators
FCC tops the agenda of regulators globally

In recent years, regulators have dramatically stepped up enforcement of anti-money laundering (AML) and CFT laws and regulations.

Today, it is not uncommon to see the US Justice Department and regulators announce multi-million dollar criminal or civil fines as settlements for AML violations.

Sometimes compliance related fines exceed many hundreds of millions of dollars with a recent judgment reaching USD 9 billion.
FCC tops the agenda of regulators globally

Record-breaking fines imposed on financial institutions

Examples of fines for AML and Sanctions violations (in USD million)

Trend of fines and penalties 2003–2014

Penalty Amount

Source: Multiple news sources

Trend of increasing regulatory scrutiny and penalty

Number of Fines

Source: Multiple news sources

Examples of fines for AML and Sanctions violations (in USD million)
Focus on financial crime risk management

Risk management guidelines related to anti–money laundering and terrorist financing issued by the Basel Committee (15 January 2014)

- Assessment and understanding of risk
- Board responsibility and governance
- Effectiveness of three lines of defense
- Transactions / ongoing monitoring
- Due diligence and customer acceptance policy
- Verification of beneficial owners and risk profiling
- MIS – record keeping, updating and reporting to supervisors
- Reporting suspicious activity and freezing of assets
- Group wide / cross border management of customer risk, management of risk, consistent policies and procedures and information sharing

AML risk tolerance, effectiveness of AML risk management framework and single client view are critical to enhance compliance standards
Key events shaping the industry standards

- FINRA, FSA (now FCA) – focus on individuals (AMLOs) for AML weaknesses
- Huge fines imposed by US regulators for sanctions and AML failures
- Regulatory audit / inspection now focus on the operations and effectiveness of the AML / FCC operations
- Regulators test skills and knowledge of staff – qualitative assessment is done by interviewing staff, amongst others
- Inspecting minutes of meetings and files to ensure that AML risks are escalated and have senior management input and oversight
- New developments from FATF perspective – TBML, new technology (mobile banking etc.), tax evasion
- January 2014 – BCBS issued guidelines on how banks should include management of risks related AML / CFT within their overall risk management framework
- July 2014 – the FinCEN proposed amendments to existing BSA regulations that would impose explicit customer due diligence requirements, including a new beneficial ownership requirement.
- FATCA implementation and impact on compliance – FATFC generally requires a financial institution to know whether a 10% owner of certain entities is a US person or not based on a self-certification provided by the entity. For most of the AML/KYC reviews, the threshold is normally 25% (for low risk customers). Additionally, FATCA monitoring for change in circumstances is not risk-based, must be monitored as it occurs and applies to all customers
- January 2015 – the FDIC released a statement encouraging institutions to take a risk-based approach in assessing all individual customer relationships rather than “de-risking,” or declining to provide services to entire categories of customers

Criminals and terrorists conduct billions of dollars in transactions each year through the formal financial sector, the informal financial sector, the trade system and cash smuggling. Despite international attempts to develop a blueprint for fighting money laundering and terrorism financing, several countries and jurisdictions – particularly some emerging and other markets – have yet to implement anti-money laundering in its true spirit.
Global, regional trends and developments
Global effort to combat financial crime …

General
Tax evasion, trade finance, new technologies, risk assessments

US
• Huge fines being imposed by US regulators for sanctions framework failures
• New CDD requirements issued by FinCEN

Europe
• EU focusing on ML/TF risk since Feb 2013, and is updating the AML Directive
• FSA (now FCA) – has fined individuals (AMLOs) for AML weaknesses

Asia
• The AML regime globally and in Asian continues to be under much regulatory scrutiny
• Key events are the mutual evaluation in Australia, Singapore, and Hong Kong, India and others

1. October 2014: FATF’s draft Guidance on Transparency and Beneficial Ownership:
   • The FATF has set international standards which require countries to implement measures to ensure that accurate information on the beneficial ownership of legal persons and legal arrangements is available to competent authorities in a timely fashion.

2. The FATF adopted the risk–based approach guidance for the banking sector which gives clear guidance on how to properly implement the risk–based approach, and is explicitly meant to be read in conjunction with the FATF Guidance on AML/CFT and financial inclusion.

FATF guidance to consider…
Regional updates and developments

- **July 2014** – The MAS released a consultation paper with proposed amendments to the MAS Notice 626. The changes aim to ensure that the AML/CFT regime is effective and in line with international best practices and FATF’s latest recommendations.

- **31 March 2015** – HKMA released a Guidance Paper for authorised institutions on anti-money laundering controls over tax evasion. The Guidance aims to enhance the effectiveness of measures to mitigate money laundering risks in respect of tax evasion.

- **June 2013** – India rectified nearly all of the technical deficiencies identified with respect to the criminalisation of ML and TF and the implementation of effective confiscation and provisional measures.

© 2015 Deloitte & Touche Financial Advisory Services Pte Ltd
Regional updates and developments

- **October 2014** – The National Coordination Committee to Counter Money Laundering (NCC) recently conducted a National Risk Assessment (NRA) to enhance the country's collective understanding of the ML and TF risks facing the country.
- **June 2014** – Amendments to AMLATFA were made with the aim of strengthening Malaysia's AML/CFT framework against criminal activities.

- **October 2014** – Japan’s cabinet approved bills to tighten rules against money laundering and terrorist financing bid to avoid being classified as high-risk and non-cooperative jurisdictions by FATF.

- **New CDD requirements** take effect from 1 June 2014 through amendments to seven chapters of the AML/CTF Rules. The new requirements introduce enhanced beneficial owner identification and verification.
- **The implementation period** is slated between 1 June 2014 to 31 December 2015. Major reporting entities are expected to be fully compliant with the new CDD rules by 1 January 2016.
Regional updates and developments

- April 2015 – The National Legislative Assembly (NLA) approved in principle three bills on the anti-money laundering agency.

- China has enacted various legislations to enhance its criminalisation of money laundering and terrorist financing
  - Repealed the old RMB–LVT/STR Rules and FX–LVT/STR Rules, and adopted new regulations which extend the reporting obligation to the insurance and securities sectors.
  - However, several deficiencies continue to remain across various recommendations and China has taken steps to enhance the effectiveness of implementation.
Impact on FCC risk management framework
Financial crime is shaping the banks’ compliance / risk programmes

**Regulatory focus**

Regulators are increasingly focussed on KYC / AML / Sanctions / Conduct issues with increased volumes of regulation and convergence amongst regulatory requirements. The focus of regulation is not on the setting of specific requirements, thresholds etc., instead the focus is upon banks:

- Effectiveness of the framework and its implementation / execution
- Understanding their risk profile
- Having a risk based approach to control
- Putting in place the appropriate governance, processes and controls

**How are banks responding**

Banks have commenced KYC / AML compliance and change programmes with a particular focus on:

i. Due diligence process
ii. Refreshed policies, procedures, processes
iii. Risk assessment
iv. Better reporting of risks
v. Single client view and owner
vi. Global KYC / AML governance
vii. Shared service centres and external utilities
viii. Remediation
ix. More prudent risk thresholds and transactions surveillance parameters
x. Documentation of decisions and senior management involvement
Framework for FCC operating model is evolving

Governance
- Risk & Management Committee
  - Group Legal and Compliance, Compliance, or Risk

Financial Crime Compliance Division
External Drivers / Regulatory Environment / Customers (behaviour, risks and service experience)
- Internal Drivers / Compliance and Risk Thresholds / Business (strategy, growth and service delivery) / Internal Audit

Financial Crime Compliance Remit – Specialisation by business segments (PB, Consumer and Global Banking)

Operations
- Operationally kept separate from FCC
  - KYC / CDD
  - Transactions, Trades Monitoring, Name screening list
  - AML Hub / CoE
  - IT / Systems

Key Drivers
- Regulatory expectations
- Cost of non-compliance
- Response to crisis or remediation
- Internal risk thresholds

Roles and Responsibilities
- AML advisory
- Sanctions advisory
- ABC advisory
- Transactions monitoring advisory
- Investigations

- Managing relationships with regulators – MLRO function
- Remediation and change
- Policy and procedures setting
- Risk identification, management & risk assessment
- Compliance monitoring and surveillance
- AML&CFT / Sanctions / ABC Advisory
- Regulatory reporting, SAR filing and internal MI
- Training and awareness

Additional Considerations
- Holistic view of remediation – effectiveness, achieving the objective
- Efficiency
- Systems and technology
- FCC, COE, CDD governance
- Crisis management
- BAU vs PMO
- Risk thresholds and variations
- Effectiveness of FCC
- Clarity of roles and overlaps
- Skills set and resourcing assessment

© 2015 Deloitte & Touche Financial Advisory Services Pte Ltd
Elements of a financial crime compliance

- Policy and procedures setting
- Advisory role
- Risk identification and assessment – risk threshold, product and client RA
- Sanctions programme
- Training and awareness
- Governance, internal dashboard reporting and MI
- Regulatory affairs – dealing with regulatory / upstream / external risk / SAR
- Monitoring and surveillance – transactions, trades, cash, sanctions
- Remediation and Change / PMO
- Resourcing and skills
Managing internal risk – escalation of FCC or AML risks to leadership, AML risk heat maps, regulatory issues, audit and risk assessment outcomes, client / product risk vs business strategy issues

Managing regulatory risk

- FCC obligations to have a sound compliance framework
- Responsive to regulatory changes and effective self assessment to remediate or prevent breaches
Financial crime risk management framework

Regulators expect financial institutions to undertake a holistic, firm–wide approach to AML compliance risk management which encompass governance and oversight, sound monitoring programme and process, staff training and comprehensive onboarding and monitoring documentation and retention.

The framework is used throughout our AML engagements as a benchmarking tool to benchmark and assess the robustness of a client’s existing framework against current and changing regulatory requirements and developments.
## Financial crime risk management framework

### Business senior management responsibility

#### Monitoring programme

<table>
<thead>
<tr>
<th>Risk assessment</th>
<th>Customer onboarding (KYC)</th>
<th>screening, risk scoring and ECDD</th>
<th>OCDD (KYC)</th>
<th>Transaction activity monitoring</th>
<th>STR investigation and FIU response</th>
<th>Disclose and exit, prevent re-entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define risk assessment</td>
<td>Identify and verify</td>
<td>Perform ECDD</td>
<td>Perform OCDD</td>
<td>Monitor transactions</td>
<td>Investigate and report suspicious activity</td>
<td>Exit customer account</td>
</tr>
<tr>
<td>Define approach to risk assessment</td>
<td>Identify new-to-bank/existing customer</td>
<td>Identify additional Key account party information</td>
<td>Scheduled or trigger-driven initiation of OCDD</td>
<td>Set transaction alert parameters and monitoring schedule</td>
<td>Create Manual STRs and Collate System Generated STRs</td>
<td>Complete and submit disclosure report and supporting evidence to FIU</td>
</tr>
<tr>
<td>Develop and maintain risk assessment</td>
<td>Identify required information for different customer/service needs</td>
<td>Perform ECDD</td>
<td>Review existing KYC data</td>
<td>Request and review supporting evidence</td>
<td>Monitor transactions</td>
<td>Assess and perform exit decisioning</td>
</tr>
<tr>
<td>Develop and maintain customer risk rating</td>
<td>Request ID and verify documentation</td>
<td>Review, approve and activate account</td>
<td>Obtain relevant approvals</td>
<td>Obtain pre-consent of suspicious transactions</td>
<td>Perform trend analysis</td>
<td>Escalate account closure decision for remedial action</td>
</tr>
<tr>
<td>Define due diligence criteria</td>
<td>Store ID and verified documentation</td>
<td>Store additional ECDD documentation</td>
<td>Change customer engagement and store KYC information</td>
<td>Evaluate and update monitoring criteria</td>
<td>Retain record</td>
<td>Maintain prohibited list</td>
</tr>
<tr>
<td></td>
<td>Perform CDD</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Identify key account party information</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Perform initial KYC (CDD)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Review, approve and activate account</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Store KYC documentation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Quality assure third party on-boarding providers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Customer risk scoring

- **Customer risk scoring**
  - Perform customer screening through existing intelligence data
  - Identify key account party information
  - Identify customer risk category (PEP and High/Normal)
  - Set due diligence criteria (ECDD and OCDD)

### Intelligence data

- Maintain intelligence lists and sources

### Sanctions screening

- Customer screening
- Payments screening

### Tailored risk based policies and procedures

- Training

### Management information and reporting

© 2015 Deloitte & Touche Financial Advisory Services Pte Ltd
Issues and expectations
Regulators continue to expect strong anti-money laundering standards, robust controls, enhanced client due diligence and suitable AML policies and procedures.

Organisational operational structures are not in sync with the fast-moving financial crime landscape.

The battle to solve financial crime is rapidly evolving into a race for the talent required to mount an effective defence.

Meeting regulatory expectations for near real-time analysis to potentially detect and prevent fraudulent activities will depend on a bank’s ability to properly leverage technology.
What are the expectations from regulators?

- Effectiveness of governance
- Robustness of KYC profiling
- Dealings with shell banks or unlicensed banks
- Anonymous, numbered accounts and/or passbooks
- Source of funds and source of wealth
- Politically Exposed Persons (PEPs)
- No face-to-face meeting with clients
- Dormant accounts
- Effectiveness of monitoring systems thresholds – periodic testing of thresholds
- Accounts that have been inactive suddenly experience large activity inconsistent with the normal practice of the client or their financial ability
- Any dealing with a third party when the identity of the beneficiary or counter-party is undisclosed
- Effectiveness of management oversight and consideration of AML / Sanctions issues at senior management / key committees
- Follow-up actions after filing of SAR – how decisions made to continue or otherwise exit the relationship

Some focus areas of regulatory inspections

- Governance: Are financial crime / AML / Sanctions issue discussed actively at your Board level?
- Focused on the importance of maintaining a “culture” of compliance and risk management. To be truly effective, the framework must be reinforced by the proper “tone at the top.”
- Trade finance compliance
- De-risking (global)
- Sanctions
- Tax evasion
- Standardisation of KYC / CDD
- Transactions surveillance and name screening / list management
- Understanding regulatory expectations amidst the regulatory diversity in Asia
- Use of technology and analytics as a step above AML framework and systems
How does ‘good’ look like?

To ensure a robust AML/CFT framework, several key weaknesses identified across different areas need to be avoided.

Further, the key fundament to a sustainable AML/CFT framework is one that is nimble, that allows for the formalisation of key practices and precedents as well as adjustments to account for new developments and requirements.
How does ‘good’ look like?

AML/CFT Risk Management Framework

Risk assessment
- Define risk
  - Identify and verify
  - Identify additional key account party information
- Define approach to risk assessment
  - Identify new-to-bank/existing customer
  - Identify required information for different customers/services
- Develop and maintain risk assessment
  - Request ID and verify documentation
  - Store ID and verified documentation
- Develop and maintain customer risk rating
  - Perform CDD
    - Identify key account party information
    - Perform customer screening through existing intelligence data
  - Conduct customer risk scoring
  - Customer risk scoring
- Define due diligence criteria
  - Quality assurance third party on-boarding providers

Business senior management responsibility

Screening, risk scoring and ECDD
- Perform ECDD
  - Set due diligence criteria (ECDD and OCDD)
- Perform CDD
  - Perform initial KYC (CDD)
  - Perform customer screening through existing intelligence data
- Identify additional Key account party information
- Request ID and verify documentation
- Store ID and verified documentation

OCDD (KYC)
- Identify key account party information
- Perform ECDD
  - Identify customer risk category (PEP and High/Normal)
  - Review and approve customer engagement and store KYC information
  - Set due diligence criteria (ECDD and OCDD)

Transaction activity monitoring
- Monitor transactions
  - Store additional ECDD documentation
  - Review, Approve and Activate account
  - Perform trend analysis
  - Obtain pre-consent of suspicious transactions

STR investigation and FIU
- Investigate and report suspicious activity
  - Escalate internally
  - Escalate account closure decision for remedial action
- Complete and submit disclosure report and supporting evidence to FIU
- Disclose and exit, prevent re-entry

Monitor transactions
- Monitor transactions
  - Store KYC documentation
  - Maintain intelligence lists and sources

Manage and maintain customer on-boarding
- Perform ECDD
  - Set transaction alert parameters and monitoring schedule
  - Review existing KYC data
  - Request and review supporting evidence
  - Obtain relevant approvals

Perform CDD
- Identify customer risk scoring
- Customer risk scoring

Monitoring programme
- Integrate and report
- Escalate (to key stakeholders)

Tailored risk based policies and procedures
- Training
  - Management information and reporting

Key Weakness to Avoid

Management oversight and involvement in decision making – especially high risk matters (clients, sanctions, PEPs, etc.) and minutes of committee meetings where AML issues are discussed

Failure to differentiate between CDD and ECDD

Systems and processes are not robust enough to deal with high risk issues or effective transactions monitoring

Failure to take action after SAR is filed or close follow up on relationships identified for exit

Weak documentation for approvals / rationale in closing and / or dealing with issues that come to the bank’s attention

Inconsistency in treatment of AML findings and as a result of process and requirements not being formalised and “ad-hoc” approach

Lack of clarity or otherwise escalation process not formalised

Timeliness in addressing remediation or recurring issues, investigation / escalations – inefficient process and exercise of judgment

Failing to record the rationale for decisions to discount false positives or transactions alerts

KYC/CDD and customer risk classifications are unclear or weak and the bank and key stakeholders do not understand the risks

Level of due diligence required is not clearly documented/ understood

“Warning signs list” and red flags are not updated regularly

Lack of standalone policies/procedures to address various specific AML risk (e.g. trade finance) and training often fails to address emerging risks
Recommendations for actions

Take a holistic approach

In practice, taking a more holistic approach means moving away from federated approaches to more centralised efforts for preventing, investigating and remediating financial crime. Here, the risk management elements that were once handled within silos are linked in an effective, organisation-wide programme. This involves seeing financial crime as a lifecycle comprising four stages — compliance, prevention and detection, investigation and remediation, and monitoring and testing — then addressing each item.

In tandem, the organisation should assess its current state, set a vision for the future state, develop a roadmap for getting there, and outline a target operating model. During this process, the organisation should search for synergies between its financial crime intelligence and customer intelligence initiatives to identify opportunities for improving customer service and adding value to the business. The more this can be achieved, the greater the economies of scale and the better the chances of cross-domain bearing fruit.

Be prepared for significant cultural change

Institutions shouldn’t underestimate the cultural and operational change programme required to take a more holistic approach to financial crime. This should begin with setting the tone at the top of the organisation and continue by working diligently toward buy-in from stakeholders, having a clear and effective communications programme, and allowing sufficient resources for training staff and managing workforce transitions.

Taking a genuinely enterprise-wide approach to financial crime therefore requires significant levels of internal communication and agreement, and can result in significant changes. For example, Deloitte has seen institutions relinquish up to 30 percent of their customers as part of programmes aimed at making their organisations compliant and resilient.
Recommendations for actions

Improve the quality of your data

The larger and more distributed a financial organisation becomes, the harder it is for it to access consistent, high-quality and standardised data. This is particularly true for institutions that have multiple technology systems because they have grown through acquisition, and those that have offices in countries such as Switzerland with restrictive data transfer laws.

In response, organisations should focus on improving and standardising data to increase their capacity to perform centralised analysis. They should also explore the use of the latest analytics techniques, which make it possible to still derive insights from unstructured information sources or data from disparate systems across the enterprise. The more sophisticated systems can not only help predict problems, they can learn as they go.

Secure the right talent – centrally and locally

The battle to solve financial crime is rapidly evolving into a race for the talent required to mount an effective defence. Our clients are experiencing a particular shortage of individuals capable of completing more analytical and critical assessments in emerging market locations, including parts of Africa, Asia, and Central and South America.

They are also finding it desirable to have strong capabilities “on the ground” close to customers, especially in locations that may be very different to the countries in which their central corporate governance and compliance teams are located.

Prepare for the future

A new framework for addressing financial crime should consider both current and future threats. As with the rise of online banking in recent years, crypto-currencies are opening up new avenues for criminals.

We are also seeing a rapid evolution in payment technologies; issues regarding commercial espionage; and a growing interest in how financial institutions can help authorities monitor money flows into and out of burgeoning sovereign wealth funds. To accommodate these trends, new frameworks should be built to expect the unexpected and allow for relatively rapid change.
Recap ...
The financial crime lifecycle

Assessing financial crime systems and policies to ensure they are efficient and tailoring systems to meet changing internal and external threats.

Assessing allegations of fraud or financial mismanagement, responding to government regulatory requests, and helping financial services organisations remedy issues and prevent their reoccurrence. This involves data assessment, e–discovery, understanding relevant laws and regulations, and undertaking cyber response activities.

Reducing financial crime incidents and identifying early issues and risks by implementing effective operational controls. The focus is on enterprise fraud and misuse management using integrated technology platforms and advanced analytics.

Acting in accordance with the requirements of relevant authorities by implementing governance structures and financial crime strategies.
A seamless and effective financial crime risk management framework needs a concerted effort across functions, with leadership from the top.

Financial institutions – Lines of defense

**Business unit**
- Relationship managers
  - Teller staff
  - In business AML

**Operations**
- Transactions surveillance
- CDD / KYC

**Geographic units and legal / compliance**
- AML / FCC specialist teams
- Regional heads
- Global heads

**Testing**
- Internal audit
- Risk assessments

**Leadership / Management**
- Board of Directors
- CCO, COO, CEO

Front line staff and their supporting administrative teams represent the first line of defense:
- Onboarding of new customers, application of Know Your Customer policies and procedures, and increasingly, performing full cycle Customer Due-diligence (CDD) activities

Provides AML advisory to and day-to-day management of the 1st and 3rd lines of defense to include AML technology applications:
- Provides assurance of controls using guidelines from UK, US, HKMA and MAS regulatory agencies and interpretation of AML regs
- Typically houses Banks' FIU; reviews High Risk clients (i.e. EDD)

- Internal testing and assurance
- Internal remediation before regulatory issues are raised

- Accountable for all FCC/AML policies, procedures, and controls
- Approves bank-wide FCC platforms and resourcing decisions
- Risk escalations
# Importance of financial crime risk management

Inadequate or poorly managed FCC programmes will increase reputational, operational, and legal risk to the bank.

<table>
<thead>
<tr>
<th>Regulatory</th>
<th>Reputational</th>
<th>Operational</th>
<th>Legal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure to meet the various regulations and expectations will subject banks to penalties and consequences. It will also mean prolonged scrutiny under the regulators’ radar – locally, regionally and globally.</td>
<td>Adverse publicity regarding an organisation’s business practices and associations, whether accurate or not, will cause a loss of public confidence in the integrity of the organisation.</td>
<td>Loss of business resulting from inadequate internal processes, personnel or systems or from external events.</td>
<td>Enforcement, lawsuits, adverse judgments, unenforceable contracts, fines and penalties generating losses, increased expenses for an organisation, or even the closure of the organisation.</td>
</tr>
</tbody>
</table>

**Wegelin & Co.**

Switzerland’s oldest bank shut down after admitting to helping American clients evade $1.2bn in taxes. Wegelin became the first foreign bank to plead guilty to tax evasion in the US and it has been forced to pay $57.8m in fines to the US authorities.

- The US allegations forced the bank to sell off its Swiss and other non-US businesses
- Wegelin is a small bank where eight partners hold unlimited liability for its operations. It has no US offices or branches and it conducted its tax evasion business in part through correspondent banking accounts at UBS the US

Source: Reuters

**Riggs**

Founded in 1836, US based Riggs Bank, which for years was known as “the most important bank in the most important city in the world,” closed its doors in 2005 due to investigations, fines, and media backlash over its sub-standard AML/Sanctions controls.

- The bank held substantial assets for Gen. Augusto Pinochet, the former Chilean dictator
- Numerous improprieties identified in some of 150 Saudi accounts at Riggs, including Saudi Royal family members
- Equatorial Guinea's dictator, Teodoro ObiangNguema Mbasago was the bank's largest client, with accounts amounting to more than $700 million

Source: The New York Times
Speaker’s profile
Radish Singh leads the Regulatory Advisory – Financial Crime, Anti-Money Laundering (AML), Sanctions and Know-Your-Customer (KYC) – practice within Deloitte Forensic in Singapore and Southeast Asia. With over 17 years of experience, Radish is a subject matter expert on advising financial institutions on financial crime. She has been actively presenting on global regulatory reform to major banks and institutions in Singapore as well as in various public forums. Her clientele currently includes major global and local banks in Singapore. She has also previously led an engagement with the Association of Banks in Singapore to revise and modernise their AML guidelines for the banking industry in Singapore. She has also advised the Institute of Banking and Finance Singapore on revising their compliance and AML industry standards modules.
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/sg/about for a more detailed description of DTTL and its member firms. Deloitte provides audit, consulting, financial advisory, risk management, tax and related services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries and territories, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte’s more than 210,000 professionals are committed to becoming the standard of excellence.

About Deloitte Southeast Asia
Deloitte Southeast Asia Ltd – a member firm of Deloitte Touche Tohmatsu Limited comprising Deloitte practices operating in Brunei, Cambodia, Guam, Indonesia, Lao PDR, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam – was established to deliver measurable value to the particular demands of increasingly intra-regional and fast growing companies and enterprises. Comprising over 270 partners and 6,300 professionals in 24 office locations, the subsidiaries and affiliates of Deloitte Southeast Asia Ltd combine their technical expertise and deep industry knowledge to deliver consistent high quality services to companies in the region. All services are provided through the individual country practices, their subsidiaries and affiliates which are separate and independent legal entities.

About Deloitte Singapore
In Singapore, services are provided by Deloitte & Touche LLP and its subsidiaries and affiliates.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte network”) is, by means of this communication, rendering professional advice or services. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

© 2015 Deloitte & Touche Financial Advisory Services Pte Ltd