Anti-Money Laundering and Counter-Terrorism Financing: From compliance to confidence

5 steps towards a new gold standard of Transaction Monitoring Systems (TMS) and reporting

The global trend of a zero tolerance to AML non-compliance

There is increasing regulatory pressure by US regulators such as the US Financial Crimes Enforcement Network and US Department of Justice towards a zero tolerance to AML non-compliance and increased emphasis on ongoing customer due diligence (OCDD) and enhanced customer due diligence (ECDD).

Global trends

Higher risks for new technologies including:

- Virtual currencies
- Prepaid gift cards
- Online gaming services
- Online money remitters

International government cooperation on AML issues such as by the Financial Action Task Force

The imposition of independent monitors, consultants and third parties as settlement requirements

AML fines against senior compliance officers

Global regulators bare their teeth

US Department of Justice

> "HSBC's blatant failure to implement proper anti-money laundering controls facilitated the laundering of at least $881 million in drug proceeds through the U.S. financial system."

BBC

> "Royal Bank of Scotland has been fined $100m (£63m, 72m euros) by US regulators for violating US sanctions against Iran, Sudan, Burma, and Cuba."

US Department of Justice

> "Commerzbank AG Admits to Sanctions and Bank Secrecy Violations, Agrees to Forfeit $563 Million and Pay $79 Million Fine."

FinCen

> The Financial Crimes Enforcement Network (FinCEN) today fined J.P. Morgan Chase Bank, N.A. $461 million for willfully violating the Bank Secrecy Act (BSA) by failing to report suspicious transactions arising out of Bernard L. Madoff's decades-long, multi-billion dollar fraudulent investment scheme."

US Department of Justice

> "BNP Paribas S.A. (BNPP), a global financial institution headquartered in Paris, was sentenced today for conspiring to violate the International Emergency Economic Powers Act (IEEPA) and the Trading with the Enemy Act (TWEA) by processing billions of dollars in transactions through the U.S. financial system on behalf of Sudanese, Iranian and Cuban entities subject to U.S. economic sanctions. BNPP was sentenced to a five-year term of probation, and ordered to forfeit $8,833,600,000 to the United States and to pay a $140,000,000 fine."

Recap: The Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act)

The *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) regulates bullion, gambling, financial and remittance services, where the conversion and transfer of physical and electronic forms of money are vulnerable to money laundering and terrorism financing.

AUSTRAC (Australian Transaction Reports and Analysis Centre) is the government's financial intelligence agency. It oversees the implementation of the AML/CTF Act and the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007* (No.1) (AML/CTF Rules).

What does AUSTRAC require?

A) Reporting entities' obligations include:

- enrolling with AUSTRAC and registering any remittance services
- implementing and maintaining an AML/CTF compliance program
- conducting Customer Due Diligence (also known as 'Know Your Customer')
- lodging Threshold Transaction Reports, International Funds Transfer Instructions and Suspicious Matter Reports
- complying with various AML/CTF record-keeping obligations

B) Customer Due Diligence is a core obligation and includes:

- assessing the money laundering and terrorism financing (ML/TF) risk posed by each customer
- collecting prescribed information on customers and identifying who owns and controls customers
- verifying prescribed element information
- performing Ongoing Customer Due Diligence (OCDD) procedures such as transaction monitoring. OCDD will help reporting entities to identify, mitigate and manage ML/TF risks that may arise from providing designated services to their customers

Consequences of AML non-compliance:

- Large fines
- Reputational damage
- Loss of business
- Loss of customer and investor confidence
- Significant legal costs

Are you doing enough to comply?

3 areas reporting entities should focus their efforts

Know Your Customer

With high error rates of 30-40% for complex entities, having a clear and consistent operating model for both KYC at onboarding and refresh needs to be a key area of focus. This should also include consideration of how all customer KYC is being refreshed.

Transaction Monitoring

Due to the complexity, data volume and systemic interdependencies, transaction monitoring systems need to be adequately tested, mapped and reconciled. Reporting entities need to increase scrutiny given to TMS systems, data quality and reporting processes.

Risk Assessments

Risk assessments must be fit for purpose, current and dynamic, tailored to the reporting entities' products and services, and considerate of terrorism. Reporting entities must be able to demonstrate a robust risk assessment methodology which determines how ML/TF risks are managed.

Transaction Monitoring — What are the key risks and challenges?

Transaction Generation	• Ineffective data capture • Poor data quality • Multiple source systems and poor integration
Core Systems	• Correct capture of data at point of sale • Complex legacy transaction host systems • Complex legacy customer account management systems
Data Transfer	• Lack of data reconciliations between systems • Data loss due to new products or system updates not captured in down stream reporting processes • Incomplete data loads • Complex ETL processes • Incomplete transfer of data between systems
TMS	• Rules are not current and dynamic in that they do not reflect the reporting entities' ML/TF risks or respond to changes in customer behaviour • TMS are not updated to respond to changes in products and services • Lack of accountability and ownership of TMS • Key person risk with regards to data flows and implementation • Expensive to implement and maintain • Lack of business understanding from the TMS vendor • Business requirements do not agree with logic interpretation • Can't retrospectively check implementation of rules • Incorrect vendor implementation • Poor data governance/IT change management
Case Management	• Inconsistent operations staff training • Inconsistent and labour intensive manual reporting processes • Manual work arounds to investigate alerts • Trend analysis is limited by poor data quality captured in case management tools

What can you do?

5 steps to success

Data governance/ IT management review

Is the TMS effectively managed and owned by the right people in my business?

Technology review

Which vendor suits me best? Review of:

- Core TMS functionalities
- Use of predictive analytics or machine learning
- Data analysis platforms: consider "Big Data" solutions and structured and unstructured data analysis requirements
- TMS service model: on-premises, cloud-based or Software as a Service

Benchmark analysis

What are my competitors doing to manage ML/TF risk?

Which vendors do they trust and why?

AML/CTF TMS Optimisation

- **Scenario Evaluation:** use understanding of current industry practices and circumstances, SME issues and investigation feedback to evaluate the effectiveness of scenarios
- **Segmentation analysis:** utilise behavioural analysis to ensure customers are alerting appropriately
- **Threshold testing:** test and set thresholds against segments
- **Ongoing metrics:** develop metrics to use on an ongoing basis. Monitoring not only the metrics themselves but trends within the metrics help detect potential areas of drift

AML/CTF TMS Testing and Compliance Review

- **Data sourcing analysis:** review data fed from the various source systems for potential gaps and quality issues that may impact transaction monitoring
- **Data quality analysis:** review the completeness, quality, and integrity of data elements used by existing and potential scenarios
- **Mapping and transformation:** analyse logic or transformation from source systems to the monitoring systems that are critical to surveillance efforts
- **Scenario testing:** evaluate the productivity and the reasonableness of existing and potential scenarios, and test the logic behind them

Contact us

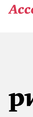
Sydney

Malcolm Shackell
Partner, PwC Australia
malcolm.shackell@pwc.com
+61 414 726 389

Priscilla Shire
Senior Manager, PwC Australia
priscilla.shire@pwc.com
+61 433 838 298

Atorina Nissan
Manager, PwC Australia
atorina.nissan@pwc.com
+61 406 884 946

Melbourne



Peter Forwood
Partner, PwC Australia
peter.forwood@pwc.com
+61 409 364 787

Will Veenhuyzen
Senior Manager, PwC Australia
will.veenhuyzen@pwc.com
+61 478 132 557

Gerard Sayers
Senior Manager, PwC Australia
gerard.sayers@pwc.com
+61 410 435 101

Access further insights at www.pwc.com.au/btbnetwork