4 August 2017

AUSTRAC shows its teeth again

Overview

AUSTRAC yesterday announced civil penalty proceedings in the Federal Court against a leading financial institution for "serious and systemic non-compliance with the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*" (**AML/CTF Act**). Acting AUSTRAC CEO Peter Clark said that the action should send a clear message to all reporting entities about the importance of meeting their anti-money laundering and counter-terrorism financing (**AML/CTF**) obligations.

This latest action comes on the back of similar proceedings, where a $45 million penalty to settle breaches of the AML/CTF Act earlier this year was enforced.

In light of this latest action by the regulator, where should you be focusing your efforts to ensure you are meeting regulatory expectations and managing your financial crime risks – particularly your money laundering and terrorism financing (**ML/TF**) risk?

Risk assessments

Too often these are 'set and forget'. Risk assessments are considered the cornerstones of how an organisation manages its ML/TF risks and the organisation must to be able to demonstrate the robustness of the assessments across all aspects of its business (including when a new product is developed or a new market entered).

Key questions to consider include:

1. Have you carried out ML/TF risk assessments for all new products, new jurisdictions, new customer types and new technologies being introduced into your business, prior to their introduction?
2. Is your current ML/TF risk assessment:
   - fit for purpose?
   - current and dynamic?
   - tailored to your organisation's products and services?
   - supported by data analytics?
   - considerate of terrorism financing?

If the answer to any of the above is 'no', then maybe now is a good time to take a fresh look at your organisation's ML/TF risk assessments and what systems, processes and controls are in place to mitigate the risks identified on a day-to-day basis.

Know your customer (KYC)

KYC remains a consistent problem for many reporting entities at both the onboarding and refresh phases. This is often due to:

- high error rates (30–40% for complex entities)
- added complexity around identifying ultimate beneficial ownership
- variations in operation models within organisations
- gaps between regulatory expectation and real-world operation
- low risk customers rarely (if ever) being refreshed.

Knowing who your customer is throughout the relationship life cycle is critical to managing the risk of ML/TF being committed through your organisation.

Key questions to consider include:

1. Have you considered and assessed the ML/TF risk rating associated with each of your customer types? Does your risk assessment of each customer type determine the level of information you collect in order to identify and verify customers, and is this reflected in the onboarding process?
2. Do you carry out a refresh of all customers' KYC information on a periodic basis, taking into account static, dynamic and external risk factors?

If the answer to any of the above is 'no', then maybe now is a good time to take a fresh look at your organisation's KYC processes, the risk assessments of your customer types, and the systems, processes and controls comprising your AML/CTF Part B Program to ensure these are aligned.

pwc

Transaction monitoring systems

For many organisations these are 'black boxes' that are not being adequately tested, mapped and reconciled. The scrutiny given to transaction monitoring systems and programs can be limited due to:

- complexities of the systems
- volumes of data
- manual dependencies
- systemic interdependences
- key person risk
- resource constraints.

Key questions to consider include:

1. Have you mapped out your transaction monitoring systems architecture, taking into account manual and automated transaction monitoring systems?
2. Do you regularly test your transaction monitoring systems to ensure the data flows are operating as expected?
3. Where automated transaction monitoring is in place, has the organisation defined the parameters/rules that generate alerts, and how frequently are these reviewed and tested for validity?
4. Where you have identified customers presenting increased ML/TF risk as a result of transaction monitoring processes, or have filed a suspicious matter report with respect to a customer, have you continued to monitor those customers to mitigate and manage ML/TF risk, including the ongoing ML/TF risks of doing business with those customers?

If the answer to any of the above is 'no', then maybe now is a good time to take a fresh look at how your organisation monitors the transactions it carries out on behalf of customers.

Reporting obligations

What you report to the regulator, both its quality and volume, is a key consideration for the regulator in assessing how an organisation is managing its ML/TF risks. As an intelligence gathering organisation, AUSTRAC prioritises the gathering of high quality data that it then provides to its various stakeholders. It also receives intelligence from other government agencies and reporting entities. If your organisation (or your customers) are mentioned in reports from other government agencies or reporting entities and you have not made any relevant reports, AUSTRAC is likely to want to understand why. Understanding your reporting obligations and providing high quality and timely data is critical.

Key questions to consider include:

1. Have you identified and articulated your reporting obligations in your AML/CTF Program, including suspicious matter reporting (SMR), threshold transaction reporting (TTR) and international funds transfer instructions (IFTI) reporting?
2. Have you provided regular training to all employees involved in the provision of designated services to ensure they are able to identify and report any potential suspicious activity?
3. Do you have adequate systems, controls and processes in place to ensure that TTR/SMR/IFTI reports are submitted to AUSTRAC within the required timeframes?
4. Do you have an internal quality assurance check and regular independent reviews to test the implementation of these processes and identify any compliance weaknesses or failures?

If the answer to any of the above is 'no', then maybe now is a good time to take a fresh look at how your organisation continues to meet its AML/CTF reporting obligations on a day-to-day basis.

Conclusion

We believe that AUSTRAC is likely to continue to take an active role in monitoring compliance and design enforcement with the AML/CTF Act and Rules. Accordingly, we encourage reporting entities to consider whether they are truly confident that their current AML/CTF framework, and the processes, systems and controls that support this, are robust enough to ensure your organisation is complying with its AML/CTF regulatory obligations.

PwC can assist you in reviewing the design and operational effectiveness of your current AML/CTF Program and its component parts, particularly those areas that are known to be on the radar of the regulator.

Let's talk

For further information on how these issues might affect your business, please contact:

Malcolm Shackell
Partner
Forensic Services
+61 (2) 8266 2993
malcolm.shackell@pwc.com

Peter Forwood
Partner
Forensic Services – Australian Financial Crime Lead
+61 (3) 8603 0664
peter.forwood@pwc.com

Priscilla Shire
Senior Manager,
Forensic Services
+61 (2) 8266 1783
priscilla.shire@pwc.com

www.pwc.com.au