

## **First Westpac, Now Afterpay: What's Next for AUSTRAC?**

**Monday, 25 November 2019**

Late last week financial institutions across Australia, and around the world, woke to the news that Australia's anti-money laundering and counter-terrorism finance regulator, AUSTRAC, had filed civil penalty proceedings against one of our largest financial institutions, Westpac, alleging that the bank had breached provisions of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (**AML/CTF Act**) on more than 23 million occasions in relation to amounts exceeding \$11 billion.

AUSTRAC's claims primarily arise from alleged deficiencies in the bank's systems and controls regarding international funds transfer instructions (**IFTIs**).

Pursuant to the AML/CTF Act, relevant entities that receive funds transmitted into Australia (from overseas correspondent banks) are required to report the IFTI to AUSTRAC within 10 business days of the instruction being received.

In Westpac's case, AUSTRAC alleges that the bank failed to comply with this obligation over a period spanning nine years and on more than 23 million occasions.

Fortunately, while the announcement may have sent shockwaves through the finance sector, Westpac have been aware of the issue for some time, disclosing in the notes to its full-year 2018 accounts and its 2019 half-year accounts that it could be fined for a failure to report the IFTIs in accordance with its obligation under the AML/CTF Act.

Provisioning for this type of event; however, is another matter entirely, and a foray into the unknown for the Board and executive team.

The only other recent and significant matter of this kind is the settlement agreed between AUSTRAC and the CBA last year in the amount of \$700 million, in relation to approximately 54,000 breaches of the AML/CTF Act and almost \$800 million in funds.

If that is the yardstick, then the potential penalty faced by Westpac for 426 times the number of alleged breaches and almost 14 times the value of funds involved could easily be, as one commentator put it, an 'extinction event'.

In response, Westpac has publicly acknowledged the proceedings, noting that it self-reported the IFTI issue to AUSTRAC and is working with the regulator to resolve the non-compliance issues.

Unfortunately, these civil proceedings are not the end of Westpac's woes, with both APRA and ASIC announcing that they too will be commencing their own investigations to determine if the AML/CTF Act failings give rise to other breaches under legislation they administer, respectively.

In other news, it has been revealed today that Afterpay may also face regulatory action for inadequacies in its financial crime compliance systems.

The results of an AUSTRAC ordered audit have revealed that Afterpay breached the AML/CTF Act because the business model was initially classified as providing 'factoring' or financing services to merchants, rather than a business providing loans to consumers.

This advice led Afterpay to focus its anti-money laundering systems and controls on the merchant end of the equation, rather than on complying with the 'know-your-customer' and other provisions of the AML/CTF Act as they relate to consumers.

Notably, Afterpay are laying the responsibility for its potential exposure to regulatory action at the feet of its lawyers, who provided the initial classification advice.

Finally, on 17 October 2019 the Federal Government introduced the *Anti-Money Laundering and Counter-Terrorism Financing and Other Legislation Amendment Bill 2019* (commonly referred to as the **AML/CTF Bill 1.5**), which raises the bar for banks and other financial sector participants when dealing with correspondent banks.

Under the new legislation, reporting entities will be prohibited from entering into, or continuing in, a correspondent banking relationship with another financial institution that permits its accounts to be used by a shell bank (i.e. a bank without a physical presence in any country).

The Bill also removes a defence previously available to reporting entities, namely that they were not reckless as to their correspondent banking relationship, and exposes regulated entities to fines of up to US\$21 million for breaches of civil penalty provisions.

If recent events are any indication, AUSTRAC is clearly on the move, intent on exposing financial crime compliance system deficiencies and driving home the message that, while possibly sitting at the technical end of the contravention scale, these breaches are nevertheless significant and will be acted upon.

Indeed, more often than not it's the failings in systems and controls (as opposed to isolated incidents of actual money-laundering etc.) that expose entities to the highest risk of litigation and regulatory action, fines, reputational damage, investor discontent and other significant costs.

Given this recent action by not only AUSTRAC, but other regulators including ASIC and APRA, regulated entities would do well to take heed and use the issues identified in each of the above cases as a roadmap for review.

For instance, now is the perfect time to review financial crime compliance systems and controls to ensure that:

- The business model has been correctly classified and compliance systems are focused on the right designated service participants;
- The organisation's overall risk identification, management, compliance and reporting framework has been updated to incorporate non-financial risks (e.g. compliance, conduct, operational, regulatory, reputation), with a particular focus on potential AML/CTF Act exposure;

- The systems and controls for capturing, monitoring and reporting international funds transfer instructions is up-to-date and compliant with existing AML/CTF Act obligations;
- The system for carrying out (and updating) due diligence in relation to correspondent banking arrangements is likewise current and compliant with existing obligations; and
- Changes pursuant to the AML/CTF Bill 1.5 are tracked to ensure the business is ready to update its financial crime compliance system, should the Bill be enacted in early 2020.

Recent cases have demonstrated the consequences of failing to act quickly when dealing with possible compliance system gaps or failings.

Should you have any queries or concerns regarding your own compliance systems and frameworks, please don't hesitate to contact us for a confidential discussion.