

PRIVACY vs. SAFE HARBOUR

– A Matter of Fact

By Tony Fitzgibbon, CEO FCS OnLine

THE TSUNAMI of AML/CTF regulations has washed over the worldwide financial landscape and Australia is right in the midst of it. Even from an implementation point of view, when Australia appeared to be behind some of the OECD nations, the reality is that it drafted and implemented the new legislation in under two years; a legislative speed of change not often seen. This speed of change is creating extreme pressure on the industry to analyse, select and implement AML/CTF compliance solutions within a very tight timeframe.

It is this pressure, and a seemingly limited range of options that appear to be driving some decision makers to the edge of acceptable risk compliance, that worries some in the industry. It could be said that for some, compliance at 'low-to-no additional cost' has become the focal point of the exercise rather than the industry attempting to eliminate, as Neil Mackrell suggests in his paper "Economic Consequences of Money Laundering", around 3.5 billion dollars¹ worth of money laundering annually in Australia that has escaped existing verification routes. By that shift of focus, the industry runs the danger of AML/CTF compliance managers and senior executives taking to the idea of (a) attempting to only achieve Safe Harbour and (b) doing so at minimal cost even if this runs the gauntlet of AUSTRAC (and potentially the Privacy Commissioner), and the risk of creating further fraudulent transactions in the marketplace. One current issue is the use of credit file information for the purposes of AML/CTF compliance. Opinion is divided over how useful this would be, and there is a degree of speculation and debate in the industry. Even with some pointed comments from the office of the Privacy Commissioner, some organisations are on the verge of opting for a potentially high risk model, with compliance deadlines looming.

From our perspective, the use of data from a credit file as an alternative means of satisfying the principles of electronic Safe Harbour, whilst on the surface appearing quite logical, appears to be restricted by the Office of the Privacy Commissioner. In a letter received 24th August, 2007 we were advised:

"The Office has previously issued advice (Credit Advice Summary 6.4) on the use and disclosure of credit reporting information in relation to AUSTRAC requirements <http://www.privacy.gov.au/publications/casw6.doc>

This advice states that:

"The Privacy Commissioner considers that it would not be lawful under the Privacy Act for a credit reporting agency to disclose information from its records to cash dealers for their use in meeting the verification requirements of the Australian Transactions Reports and Analysis Centre (AUSTRAC) (formerly known as Cash Transaction Report Agency (CTRA)). It is considered that the authority contained in the AUSTRAC regulations could not be interpreted as conferring an authority upon a credit reporting agency to disclose in the way described in s. 18K(1)(m). Further, there is no corresponding use provision enabling a credit provider to use a credit report for AUSTRAC verification requirements."

The office does not consider that there are any provisions in the AML/CTF 2006 Act that would alter this advice....."

Further to this, in a submission to the Australian Law Reform Commission (ALRC Discussion Paper 72 Review of Australian Privacy Law), it was stated by a credit reporting agency:

"...electronic identity verification has been a significant focus of attention in the development of the AML/CTF Act and that the use of credit reporting information for identity verification has a clear public benefit in protecting consumers and business from harm. The company sought 'urgent measures to permit the use of credit reporting data in electronic verification for the purposes of AML/CTF laws'."

In one of its responses, the ALRC commented:

"The ALRC recognises the force of arguments in favour of allowing credit reporting information to be used and disclosed for identity verification and related purposes. Credit providers are concerned that, while new statutory identity verification obligations have been imposed under the AML/CTF Act, they are not authorised to obtain electronic data that would enable them to comply efficiently. In particular, the ALRC understands that credit reporting information is potentially an important source of date of birth, which is not generally available from public sector databases."

On the other hand, the AML/CTF Rules provide considerable flexibility with regard to the means of identity verification."

¹. "In Australia, AUSTRAC recently commissioned a very interesting study that suggested that between A\$1 billion and A\$4.5 billion may be laundered in and through our jurisdiction annually, with the most likely figure being around \$A3.5 billion". Economic Consequences of Money Laundering – Neil Mackrell

Verification of information collected about a customer may be based on: reliable and independent documentation; reliable and independent electronic data; or a combination of these...

... There are arguments that, if existing electronic sources of personal information are insufficient to meet the needs of reporting entities, the Government, having imposed identity verification obligations, should look to facilitate access to government databases before looking to private sector databases, such as those held by credit reporting agencies...

... The ALRC needs more information about the risks, benefits and possible alternatives before making any recommendation that the use and disclosure of credit reporting information for identity verification should be authorised. The issue needs to be considered in the light of many recent developments, including the proposed Document Verification Service and the due diligence requirements of financial services legislation and other similar statutory identification obligations. Ultimately, however, the balance between privacy and the need to combat money-laundering and the financing of terrorism in this context is a policy decision."

This is a lengthy process!

I am of the opinion that it is far better, as the ALRC puts it, that "the Government having imposed identity verification obligations, should look to facilitate access to government databases before looking to private sector databases, such as those held by credit reporting agencies."

There are many such databases with the appropriate level of personal information necessary for reliable identity verification, and with enough due process and controls to ensure a high degree of accuracy and authenticity. Aside from the matter of privacy, a major flaw in using a credit file is that there are no real quality control checks of the validity of the information contained in the file. In other words, someone could create a new-to-bureau file with false identity information, wait for a given period of time, and use those very same details on an account opening or credit application. No doubt there could be a raft of checks and balances to counter this, however why go to this effort when, as the ALRC indicates, more reliable sources of information can be made available for the purposes of AML/CTF?

If Government is inclined to legislate to make DOB data available for AML/CTF compliance in line with the philosophy

behind the ALRC proposal, there are other primary sources which would be much better suited for this purpose and meet the requirements of independence and reliability, namely:

- (a) Electoral Roll
- (b) Birth registrations

Electoral Roll

Part of the information held on the electoral roll is DOB information. It is however not generally available. It could be made readily available, with appropriate legislative support (under the Commonwealth Electoral Act 1918 and privacy legislation)

Birth Registration

The NSW Registry of Births Deaths and Marriages has collected DOB information from all states in Australia, except Tasmania and Northern Territory which, we understand will shortly be made available. The cost to access this information is high but the file requires very slight modification to enable it to be used for AML/CTF Safe Harbour verification.

In conclusion, the AML/CTF legislation should *not* be regarded by responsible businesses in Australia as just a compliance issue; rather it should be regarded as part of an ongoing process of monitoring financial transactions to ensure that money launderers and terrorist financiers have the least possible chance of getting through the systems and processes designed to detect and stop such activities.

Identi-Check® for AML has been designed for the unique requirements of the Australian market. In essence, *Identi-Check® for AML* is designed to assist organisations achieve AML/CTF compliance by allowing them to make informed reporting decision based on their risk assessment program. The solution can be rapidly deployed utilizing multiple delivery options and is designed to be future proof, giving organisations the confidence that as their compliance requirements change, so too can the Electronic Verification solution they have invested in.

To enable organisations to fast-track their EV requirements, FCS Online has partnered with a global information technology services and solutions company Unisys to deliver *Identi-Check® for AML* as a hosted service. Unisys is a recognised leader in both data and physical security solutions, ranging from biometrics to secure data centres. ■

For more information on *Identi-Check® for AML*, you can contact:

Mathew Cagney – FCS OnLine
Phone: 02 8912 1000
Email: info@fconline.com.au



Robert Dewar – Unisys
Phone: (02) 9647 7777
Email: robert.dewar@unisys.com



At the date of printing neither The Minister for Justice & Customs nor the Privacy Commissioner have amended provisions contained in this advice.