FSU AUSTRALIA
www.fsunion.org.au

Jackie Morris
A/Secretary Legal and Constitutional Affairs Committee
Department of the Senate
Parliament House
Canberra ACT 2600
legcon.sen@aph.gov.au

Dear Ms Morris

Re: Inquiry into the Anti-Money Laundering and Counter-Terrorism Financing Bill 2006

The Finance Sector Union of Australia (FSU) welcomes the opportunity to contribute to the inquiry process for the Anti-Money Laundering and Counter-Terrorism Financing Bill 2006.

The FSU represents 60,000 members employed in the finance sector across Australia. Our members work for many of the 'reporting entities' that provide 'designated services' that will be monitored by the proposed measures.

Given the large amount of complexity and the short timeframes involved the FSU has commented on broader issues related to the potential impact on employees in relation to training, liability and their relationship with customers and the need for a public awareness campaign around the proposed requirements. In addition, some potential privacy and data security implications related to the trend for financial services companies to perform work 'off-shore' are discussed.

We believe the Government is effectively requiring finance sector staff to help with law enforcement activity but is not implementing mechanisms to ensure that these staff are given enough resources to properly carry out these activities – decisions about national security will effectively be influenced by commercial pressures of understaffing and a sales culture.

We believe the Australian Government can (and should) play a role in helping to encourage a culture of compliance with the letter and spirit of the law whilst supporting staff in dealing with the pressures they face.

Training

The FSU supports the general principles behind the Bill, however, FSU's main concern is ensuring that finance sector staff receive adequate training to comply with the new requirements and that finance sector staff are not unfairly burdened. Finance sector staff are already subject to numerous regulatory requirements and internal procedures that are often performed under tight timeframes and sales targets pressures. Currently the average salary for a bank teller is $35,000[1] which is low given the levels of responsibility involved – this Bill will only increase the amount of

[1] Hays 2006, *Sector Commentary Banking & Finance.*

responsibility and pressure on a workforce that already does over 1,000,000 hours of overtime every week.[2]

Our concerns regarding training around new finance sector requirements can be illustrated by reference to how the Financial Services Reform Act (FSRA) was implemented in numerous banks and insurance companies.

Unfortunately, in many companies we witnessed a further intensification of work for staff without corresponding adjustments to staffing levels or sales targets. Some companies even went so far as to use the FSRA introduction as an excuse to increase sales pressures on staff, a process that would seem to run counter to the intent of the legislation to minimise inappropriate sales.

FSU conducted a survey regarding the impact of the FSRA on training and workloads. The survey was distributed to all FSU Members and results from 1,125 finance sector workers were collated in early 2004.

The majority of respondents (65.2%) said that FSRA had made their jobs harder or more complicated, and 63.6% of respondents claimed that some tasks now take longer to complete than they did prior to the FSRA.

88.2% of respondents who work to targets stated that targets had not been adjusted to reflect workload changes. Of those who stated their targets had been adjusted, only 31.6% believe they have been adjusted appropriately. Of that 31.6%, approximately half in retail branches believed their targets weren’t adjusted appropriately.

To help the Government achieve the aims of the current Bill it is essential that these new requirements are not simply added onto existing workloads without appropriate resources and recognition of the extra work involved. Ultimately if staff are unduly pressured by time constraints they may not file reports that should be filed and the aims of the Bill will be undermined.

Liability and reporting

Our general understanding is that individual staff members would not be liable “in relation to anything done, or omitted to be done, in good faith by the first person, officer, employee or agent”.[3] This is welcome and necessary; however, we hold concerns regarding how staff members will be treated in relation to any transgressions that might occur. Protection from strict legal liability is one thing but it does not protect an employee from other forms of punitive action from their employer, if they fail to follow the requirements of the Bill.

Our concerns relate to ensuring that employees are not held responsible if they are not provided with adequate training to carry out the new requirements that will be imposed upon them. Another example from the FSRA illustrates our concerns. An FSU member working in a banking environment was assessed online. She did her training, completed the assessment and failed. The training program did not tell her why she failed, so she just kept putting in different combinations of answers until she passed. Thousands of finance employees would have undertaken this method of assessment and would have been considered to have received adequate training when in fact they hadn’t. This situation highlights the divergence between a corporation achieving technical compliance and staff being capable of properly understanding the aims and requirements of any new regulatory regime.

---

[2] FSU 2005, *The Finance Sector Workforce Report* – Based on ABS statistics.
[3] Section 235(1) *Protection from liability*

Relationships with customers

The Bill will greatly expand the law enforcement role of financial institutions and this will impact on the relationship that staff have with customers. Many customers will not welcome the increased amount of surveillance that finance sector staff are expected to conduct when interacting with customers. Many finance sector staff report that they enjoy getting to know and interacting with customers[4] but are often pressured to try and sell products to meet sales targets which is often not appreciated by customers. Unfortunately, the Bill is only likely to increase any tensions in existing relationships with customers.

It should also be noted that the overwhelming majority of customers are not involved in money laundering or terrorism yet all customers will be effected by these measures. We appreciate there is no simple way to resolve this tension but we believe it highlights the importance of ensuring that staff have adequate training and time to carry out these procedures and that the public fully understand why the Government has imposed these obligations on finance sector staff and ultimately customers.

Public awareness

The FSU is also cognisant of the fact that reporting entities will have a greater ‘law enforcement’ role that some customers may perceive as intrusive or invasive. To minimise any potential customer hostility in this regard we would encourage the Committee to ensure that adequate public awareness measures are put in place before the Bill is fully implemented.

Privacy and data security

One issue that may begin to impact on the operation of the Bill is the increasing trend for finance sector companies to undertake many of their processes ‘offshore’. Customers have already expressed strong concerns regarding provision of their personal data to offshore locations,[5] given that the Bill will increase the amount of personal data being collected it is likely that customers will be even more uneasy and distrustful about providing this information.

There would also seem to be an inherent tension between the aims of the Bill and the rush towards offshoring of finance sector processes. The Bill aims to increase the level of security and monitoring that exists in our finance sector, however the experience of offshoring has shown that many overseas jurisdictions have greater dangers in relation to security of data[6] that is likely to impact on the effectiveness of any monitoring regime that may be put in place.

Offshoring introduces inherent risks that are not sufficiently considered by this Bill or any other existing legislation.

Review and oversight

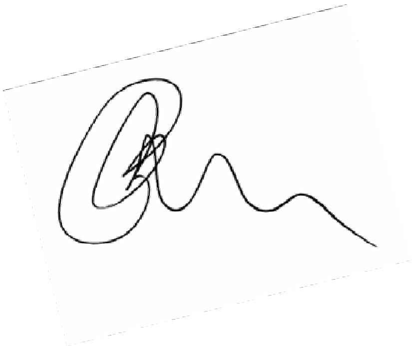
Given the importance of these measures and the impact they may have on staff we would encourage the Government to ensure that their voices are included in any

[4] Essential Media Communications 2006, *Focus groups report*
[5] McNair Ingenuity Poll, May 2006 - *Attitudes to Offshore Labour*
[6] See attachment A for a number of examples of breaches of financial data security involving offshore locations.

review process. We believe this will help to ensure that the aims of the Bill are achieved without unfairly burdening staff and impacting on consumers.

If you have any questions in relation to this submission please contact our National Communication and Policy Manager, Rod Masson, on (03) 9261 5330.

Yours sincerely



Paul Schroder
National Secretary
20 November 2006

Offshoring – Data/Privacy breaches

International bank HSBC hit by Bangalore breach

June 27, 2006

A security breach at international bank HSBC's offshore data-processing unit in Bangalore has led to a theft of £233,000 pounds ($424,832).

A 24-year-old worker at the HSBC operation has been suspended after being accused of accessing confidential account information and passing it on to criminal associates in the United Kingdom.

http://news.com.com/International+bank+HSBC+hit+by+Bangalore+breach/2100-1029_3-6088474.html

Indian call center worker arrested

September 7, 2005

NEW DELHI--Police have arrested a call center worker for alleged theft of personal customer information that the firm was handling for its clients.

The arrest was made after the call center, Saffron Global, reported the matter to the police. Company officials said the worker was found copying personal information about customers onto a compact disc.

http://news.com.com/Indian+call+center+worker+arrested/2100-7348_3-5852487.html?tag=nl

U.K. watchdog targets data breach

June 23 2005

U.K. banks have been warned they face prosecution for breaching the Data Protection Act after a call-center worker in India sold bank account details of 1,000 U.K. customers to an undercover reporter.

The security leak was discovered following an investigation by a newspaper reporter from The Sun, who was able to buy bank account, credit card, passport and driver's license details of U.K. bank customers for just 4.25 pounds (about $7.75) each.

The call center worker in New Delhi also told the reporter he could supply confidential data from 200,000 accounts a month. The newspaper handed a dossier with all the details to the City of London police.

http://news.com.com/U.K.+watchdog+targets+data+breach/2100-7348_3-5759218.html

Indian call centre staff in $350,000 Citibank theft

11 April 2005

The Indian offshore outsourcing industry has been rocked by the revelation that call centre workers in Pune have been arrested for allegedly looting $350,000 from the accounts of Citibank's US customers.

The three staff are former employees at Indian business process outsourcing (BPO) firm Mphasis, which runs call centre services for Citibank's US customers in Bangalore and Pune. Nine other gang members were also arrested.

http://www.silicon.com/research/specialreports/offshoring/0,3800003026,39129426,00.htm

See also **Australian Broadcasting Corporation** (ABC) 2005. "*Your Money and Your Life"*,4-Corners (15/08/2005).