

ABS Financial Crime Seminar
Thursday, 12 July 2013
Welcome Remarks by Mr Samuel Tsien
Chairman, ABS / CEO, OCBC Bank

Mr Lee Boon Ngiap, Assistant Managing Director of the Monetary Authority of Singapore
Distinguished Guests
Fellow Bankers
Ladies and Gentlemen

Good morning.

On behalf of the Association of Banks in Singapore, welcome to this year's Financial Crime Seminar.

This is the 10th year running that the ABS is organizing this seminar, and I am pleased to note that the participation at this event has continued to grow from year to year. This year, we have a record of 540 participants. The success of this seminar indicates the increasing attention that banks are paying to issues concerning financial crimes, which include money laundering, terrorist financing and more recently, cybercrimes and tax evasions. As an industry, this is an area which we should and would need to continue to work together in collaboration with the various governmental agencies to strengthen our defences.

During the height of the internet bubble, many naysayers were predicting the demise of conventional banks. They likened "brick-and-mortar" banks to dinosaurs and claimed that they would be marginalized by technology start-ups and pure internet banks. Well, reality had unfolded otherwise. There is however one key point that was clear, then and now, that while it was argued whether customers would like their banks in their original forms or not, they certainly TRUST them.

The customers' trust and confidence in a bank is crucial to its viability as a going concern and, for that matter, to the entire financial system. Apart from the sense of security conveyed by physical branches and solid balance sheets, customers trust banks because of their reputations. Different banks may have different reputations, but as a baseline, customers expect their banks to act responsibly, among which it includes putting in adequate safeguards and controls to ensure that the financial system is not used by criminals or terrorists as a conduit for channelling funds or laundering money. They also expect that the bank's systems are resilient enough to hold up to external attacks, such that their wealth and the records of their wealth with the bank are safe.

A bank that fails to put in sufficient controls which consequently result in security lapses will suffer both financial and reputation loss. The high profile cases of regulatory sanctions against banks that were alleged to have assisted tax evasions and money laundering, as well as recent news about the attacks on the computer networks of a few major banks in South Korea, clearly illustrate that the risks are real. It was reported in the news that the fines imposed on banks topped US10bn last year, of which 3 banks alone were fined over USD3bn for money

laundering violations. We are not talking pocket change here. Apart from these staggering sums of penalties, it takes a long time to restore customers' confidence in the institution once it had been eroded.

The compliance of banks in Singapore with international standards regarding AML and CFT is also key to the continued success of Singapore as a major financial center. With financial services accounting for more 12% of our Country's GDP and contributing more than 180,000 higher value added jobs, it is not hard to see why Singapore needs to maintain its top reputation as a 'clean' financial center. Only with a solid reputation built on the foundation of trust and integrity can Singapore continue to be an international financial center and tap into the global opportunities in asset management and many other financial services.

It is therefore important that as an industry, we continue to work together with the regulators and the law enforcement agencies, to stay abreast of current developments and continue to guard against financial flows associated with corruption, terrorism, weapons proliferation, and most recently, tax crimes which was added as to the list of money laundering offences.

At the same time, we would also need to find ways to do so in a cost effective manner, given the rising operating costs that banks have to incur to comply with the increasing, and increasingly complex, regulations. The Inter Government Agreement (IGA) between the US and its partner jurisdictions for FATCA including Singapore, is a good example of how the complexity and cost of implementing regulatory requirements can be reduced through closer collaboration between the private and public sectors. Another example is the recent formation of the ABS Standing Committee on Cyber Security. Together with MAS' participation, this committee shall serve as a platform for banks to share cyber intelligence, discuss major cyber security incidents, and collectively develop solutions to counter emerging cyber and technology security issues.

On that note, I would like to express our appreciation to the Monetary Authority of Singapore for facilitating the signing of the IGA with the US which, as I said, would significantly reduce the complexity and cost of implementing the new FATCA rules. I would also like to thank Mr Lee Boon Ngiap, assistant managing director of the MAS, for kindly accepting our invitation to deliver the keynote address for this conference, and the various prominent speakers for joining us to update us on the recent developments in the areas of money laundering, risk assessment, cyber crimes and financial frauds. Their insights, experience and expert knowledge will be invaluable to us as we continue to strengthen our capabilities to comply with the recent changes in regulations and, more importantly, address the evolving threats targeted specifically at banks and our customers.

With that, I wish you all an informative and fruitful conference.