ABS Financial Crime Seminar

13 July 2016, Raffles City Convention Centre

Keynote Address by Mr David Chew, Director, Commercial Affairs Department

Distinguished guests, ladies and gentlemen, a very good morning to everyone. Let me first thank ABS for inviting me to share my views on money-laundering, terrorist financing and other challenges facing our banking industry.

The ABS Financial Crime Seminar is perhaps the single most important event on your annual calendar where professionals from the banking community gather to take stock of current challenges and trends in the areas of anti-money laundering and counter-terrorism financing. Looking at the programme, I see that ABS in its customary efficient manner has brought in illustrious speakers, including not just practitioners from Singapore but also experts from the United States of America and the Peoples' Republic of China. Thank you for being here, we have a lot to learn from each other as we interact and exchange our different perspectives to common challenges in a fast changing world.

The flow of money is the life blood of a open economy like Singapore. Thomas Friedman in his 1999 book, The Lexus and the Olive Tree, described investment capital as an "electronic herd [that] votes every minute of every hour of every day". Money flows through our financial system only because the electronic herd trusts it. Lose that trust and the life-giving flow stops. Those of us who lived through the 2008 global financial crisis witnessed first-hand what happens when financial markets seize up and money stops flowing. Whilst markets may recover in the long run, some people and banks may not. The financial crisis showed that as intermediaries between capital seeking returns and businesses looking for capital, all of you and the financial institutions that you represent play an important role in the orderly flow of money. This flow of capital does not happen by chance. We all work hard to make this happen. Government provides the legal and physical, infrastructure that links us reliably to the rest of the world, a strong domestic economy with a stable currency and a system of clear, legally enforceable rules that everyone has to play by. The financial institutions creates the markets that form, float and sell investment products of dizzying variety which turns invested funds into productive capital, financial intermediaries like brokers, money market houses, hedge funds and market makers facilitate the trading and hedging of risk and profits and a forex market allows investors to convert and repatriate their profits in a currency of their choice.

As the party who intermediate these capital flows, financial institutions are particularly susceptible to being abused by money launderers, so every industry player must be

vigilant against this threat. As a clean and trusted financial centre, Singapore has a zero-tolerance policy for any abuse of its financial system. This resolve to uphold the integrity of our financial sector was demonstrated recently when robust regulatory and enforcement action was taken to shut down a bank in Singapore for severe AML breaches and 6 members of the bank's senior management and staff were referred to the Public Prosecutor, who has charged 2 persons, including one banker, for their involvement in a complex international money laundering case.

On this sobering note, I hope to identify 3 trends that bankers would do well to pay heed to, namely 1) the use of corporate structures to conceal beneficial ownership of financial transactions, 2) the Spectre of Terrorism abusing the financial system to fund its activities and 3) E-commerce enabled crime happening at the click of a mouse.

Corporate structures and beneficial ownership

"Sunlight is said to be the best of disinfectants; the electric light the most efficient policeman" Justice Louis Brandeis.

Criminals rarely leave their calling cards at a scene of a crime. Financial criminals are sophisticated and they often create and operate corporate vehicles that transact internationally. Their intent is to move money across various jurisdictions thereby preventing law enforcement authorities in any one jurisdiction from obtaining all the relevant information about that corporate vehicle.

There is growing international momentum to improve the transparency and integrity of financial flows, so as to deter and prevent the abuse of corporate structures by criminals. In fact, G20 leaders have declared this as a 'high priority', as so has the Financial Action Task Force, FATF.

For this highly important area of work, financial institutions play an important role as gatekeepers to provide critical information on beneficial ownership. You must continue to improve your systems and processes to ensure that accurate information can be provided in a prompt manner to law enforcement authorities and regulators. In practice, financial institutions rely heavily on the information received from their clients to verify ownership information. Doing so on simple company structures as well as publicly held entities is not complicated. However, identifying complex ownership structures which are located overseas is a challenging area. The global push for greater transparency of information will create a level playing field and increase accessibility of such information on a global scale.

When coming across a suspicious transaction, financial institutions are required by law to red flag it and file a Suspicious Transaction Report or STR with the Suspicious Transaction Office or STRO of the Commercial Affairs Department. Such information from your institutions allows us to paint a comprehensive picture of potential illicit money flows in as well as out of Singapore. In 2015, we received about 10,000 STRs from the various banks in Singapore.

STRO's Outreach

Let me assure you that the flow of information is intended to be a two-way exchange. Not just from financial institutions to us but also from us to you. In 2015, STRO revamped the CAD website to create a "one-stop" location for guidance for all sectors on STR reporting. The webpage now groups STR filing guidance according to sectors. STR filers can conveniently access red flag indicators for their sector, AML/CFT regulations and guidance issued by their respective regulators, Frequently Asked Questions on filing STRs, STR forms and step-by-step instructions on completing the STR forms. It also provides users of our online STR filing platform (STROLLS) with quick reference guides to obtain feedback on the STRs they have filed, in real time.

In 2015, STRO rolled out new publications with detailed red flag indicators and typologies, for example, updated red flag indicators to detect Terrorism Financing, Proliferation Financing, Trade-Based Money Laundering, Unlicensed Money-Changing and Remittance Businesses and Money Laundering using Trust Companies. We hope that financial institutions find these advisories useful. Do give us your feedback if there are other types of information that you might find useful.

Spectre of Terrorism abusing our financial systems

Terrorism is no longer limited to vulnerable geographical zones, as attacks in Paris, Jakarta and Dhaka have shown - it has morphed into a global threat. As the influence of the Middle Eastern terror group Islamic State of Iraq and Syria or ISIS grows, the threat to Singapore also increases. In 2015, Singapore was identified as a possible target for attack by an ISIS post on social media (http://www.straitstimes.com/singapore/isis-social-media-post-in-may-cites-singapore-as-possible-target). To tackle this terrorism threat effectively, we need to ensure that we have a multi-prong approach, including detecting, preventing and deterring the funding of terrorism.

Singapore takes a very serious view of any support for terrorism-related activities including terrorism financing. The CAD recently demonstrated that it will take firm and decisive action against any person who donates or possesses funds for terrorism-

related purposes, even if the funds are not intended for terrorist acts in Singapore. In April 2016 the Internal Security Department detained 8 radicalised Bangladeshi nationals under the Internal Security Act. . A month later, the Commercial Affairs Department charged 6 of these detainees with Terrorist Financing offences under the Terrorism (Suppression of Financing) Act. Four of them have pleaded guilty to these charges and they have been sentenced to imprisonment of between 24 months and 60 months. This is Singapore's first prosecution and conviction under this Act. This case is a timely reminder that we must not let our guard down in our fight against terrorism and terrorism financing.

Apart from terrorist fomenting acts of terrorism here or overseas, there may be individuals in Singapore who are sympathetic to terrorist causes and are open to donating or raising funds to support terrorist groups overseas. Detecting TF activities is challenging as it often involves smaller amounts of money as compared to the laundering of criminally-derived funds. In the recent case involving the six Bangladeshi nationals, the amount raised was a relatively small, $1,360. The monies were from legitimate sources – namely the salaries of the Bangladeshis. The mode of transfers between members were conducted in cash and through bank accounts. The monies were first raised in cash and the bulk of the cash were deposited into the leader and treasurer's bank account. This was eventually consolidated in the treasurer's bank account by internet banking transfers. This shows that our banking system can be used as a conduit by terrorist for fund raising activities and detection of TF can be very difficult, but we nevertheless need to be vigilant.

STRO in collaboration with the relevant law enforcement agencies have developed TF-related red flag indicators, and these indicators are published on our online system, STROLLS for reference by all reporting entities. The red flag indicators are meant to help reporting entities identify suspicious transactions linked to terrorism financing. To ensure its relevance, STRO continuously updates these indicators based on new developments and feedback received. For example, STRO updated the red flag indicators to incorporate ISIS-specific data. On the international front, FATF has embarked on a project on 'DETECTING TERRORIST FINANCING: RELEVANT RISK INDICATORS' which is a topic that our first speaker, Mr Paul DeGarabedien will be covering. Paulie is the co-Chair of the FATF Working Group that produced the paper. We are happy to have him here with us. As a member of FATF, Singapore has provided various inputs to the project paper. While the paper will not be released to the general public we will work with ABS to circulate it to STR FILERS on a restricted basis.

Crime at the click of a computer mouse

Financial Scams

I note the inclusion of the topic on Financial Scams in this year's Seminar agenda. This focus is timely as E-commerce enabled crime has been increasing at an alarming rate in the past 4 years. Financial Scams are one area that we ignore at our peril. Criminals are a savvy bunch, you can be sure that right now, they are cracking their heads on the next big scam. They are adept at using technology to get a better return on their investment, for example the recent DHL scam uses an automated voice system that ensures that only victims who respond to their calls are routed to a human operator. That was in May this year, in June the automated voice system started impersonating a SPF officer in order to steal the victim's personal information.

Like wolves in sheep's clothing, instead of fictional products like 'prime bank' instruments, more scams involve legitimate financial instruments. These include offering fund management services, trading in securities, leveraged foreign exchange or investment in companies with promises of an upcoming listing in overseas stock exchanges. Obvious red flags like outlandish returns in excess of 100% are becoming a thing of the past. Instead, people are being enticed by promises of profit sharing or lower but still attractive returns spread out over a length of time. What does this mean for all of us? Differentiating genuine investment schemes from fraudulent ones is becoming increasingly difficult.

CAD is concerned about this growing threat. In response, a dedicated Investment Fraud Division was set up when CAD was re-structured in 2013. Having dedicated investigators focusing on investment fraud allows us to build up the skills and expertise required to deal with increasingly complex and sophisticated scams.

We will pursue such scams with vigour. But the solution cannot rest solely with the CAD. Investors need to play their part. Unfortunately, these investors are often blinded by greed especially when they see other investors receiving their promised returns. When they start receiving their initial returns, they are persuaded by the criminals to plough more money into the scam, not realising that they are stepping into a trap. When the trap is sprung and the promised returns dry up, CAD starts receiving complaints from these investors. The trouble is, by this time, the scam has almost certainly run its course and the money has been squirrelled safely out of Singapore. Only a fraction of the invested funds may be recovered, if at all.

How can financial institutions help improve this situation? Financial intelligence through the suspicious transactions reporting regime is crucial in uncovering scams while they are still in the early stages of their life cycles. Many fraudsters use

corporate entities to operate and market their investment scams. Investors are instructed to pay into bank accounts set up by local money mules. In other words, proceeds of crime are channelled through the banking system. Rigorous Know Your Customer or KYC programs and vigilant transaction monitoring will raise red flags. For example, where there is a high turnover of funds in a corporate bank account with little or no funds being channelled towards the company's stated business activity. That information in turn could be critical in helping us determine whether an investment scheme is fraudulent and needs to be stopped in its tracks.

Fin Tech

Online Peer-to-Peer lending platforms that seek to by-pass financial institutions by matching capital directly to businesses without the KYC and CDD checks by an investment banker have resulted in complaints to the CAD when such investments go sour.

Financial institutions offer innovative technological solutions to stay connected and relevant to your increasingly mobile and digitally-savvy customers. Advances in technology give customers access to banking services without a human interface on a 24/7/365 basis. This enables the customer to undertake banking transactions anytime and anywhere in the world. However, this also enables a criminal who has stolen your password or banking token to undertake unauthorised transactions with similar ease.

The growing awareness of the risks presented by Fin Tech should not stop us from adopting and adapting it to meet a changing marketplace. However, our financial systems needs to develop compliance policies and procedures that prevent it from being abused by criminals. Fin Tech is a fast developing area and we encourage you to perform regular reviews and risk assessments on products and services to identify existing or potential risks and to put in place controls to address such risks.

2016 Bangladeshi Bank Heist

Your customers are not the only ones at risk. FIs themselves can be targets if we are not vigilant.

In early February 2016, the Bangladeshi Central Bank suffered a cyber-attack on its computer systems. As a result, USD 101 million was stolen from its account at the Federal Reserve Bank of New York. 35 unauthorised payment instructions were generated and transmitted to the Federal Reserve Bank of New York where Bangladesh's foreign currency reserve was kept. 5 payment instructions amounting

to USD101 million were processed while the other 30 instructions amounting to USD850 million, were blocked by the Federal Reserve Bank of New York.

This heist was traced to hacker penetration of the Bangladeshi Central Bank's SWIFT (Society for Worldwide Interbank Financial Telecommunication) Alliance Access software. Malware in the bank's computers caused it to issue unauthorised SWIFT payment messages with valid SWIFT credentials of Bangladesh Central Bank employees.

Financial Institutions are all reliant on technology to conduct their business. The heist at the Bangladeshi Central Bank is a fitting reminder of the risk of cyber-attack by criminal elements. We need to be vigilant. Your staff must be alert to the risk of cyber-attacks on their bank as the human element is often the weakest link in a bank's cyber defences. Your computer security teams should regularly evaluate and patch vulnerable software to protect your IT environment. You may also wish to consider restricting internet access from the SWIFT payment system to minimise the likelihood of compromise.

International Wire Transfer Fraud

Before I end my speech, I would like to do so on an optimistic note that illustrates what can be achieved if we work together.

In 2012, CAD detected a spike in International Wire Transfer Fraud offences where businesses overseas were defrauded into paying the criminal instead of the rightful creditor. As a result of these foreign predicate offences, money was laundered through bank accounts in Singapore. We reached out to the banks through ABS to alert financial institutions of this trend. Working with the banks, we stepped up our law enforcement efforts. By promptly filing STRs, the banks played a critical role in enabling us to detect these ML offences. Where the tainted funds were still in Singapore, the receiving bank's co-operation was sought to swiftly seize the funds.

Banks also played a part in our massive and sustained public education campaign to warn the public against being a money mule and abusing their bank accounts to launder money. CAD distributed crime prevention brochures for customers of banks and remittance agencies who were opening new bank accounts and/or executing unusual remittances. Banks also placed anti-crime messages on their websites and ATM screens.

As most of the money mules are recruited via online social networking websites, CAD purchased advertising space on popular social media websites, to warn the public of the adverse consequences of being a money mule. The money mule

problem was also highlighted on the Crime-Watch TV series. Working with the media, we publicized such cases, including our prosecutions of local money mules, to help the message sink in.

This unprecedented approach saw the number of cases dropping from a peak of 212 in 2013 or 58 cases in 2015. This success could not have been achieved without the hard work and effort of our financial institutions, all of you. Thank you!

Conclusion

Your attendance here today is a testament to the financial institutions commitment in the fight against financial crime. Singapore prides itself as a clean and trusted financial centre. To maintain Singapore's hard earned reputation, you have an important part to play as a bulwark against illicit funds flows. With robust compliance regimes and strong internal processes in your financial institutions, you are well-positioned to overcome the challenges financial crime poses to us in Singapore.

On this note, I hope you all have an enjoyable and stimulating seminar. Thank you.