Speech by Mr Chua Kim Leng,
Special Advisor, Financial Supervision Group
Monetary Authority of Singapore,
at the AML/CFT Industry Partnership Dialogues, 14 May 2018

1 Good morning Mr David Chew, Director, Commercial Affairs Department, distinguished guests, ladies and gentlemen. I am delighted to join you today at this important milestone for the AML/CFT Industry Partnership, ACIP in short.

2 Let me begin by first thanking the ABS for organising this event and members of the ACIP for their wholehearted support over the past year. I'd like to echo David's comment that ACIP has achieved a great deal in its first year. From a risk management perspective, it has contributed significantly to deepening the industry's collective understanding of money laundering and terrorism financing (ML/TF) risks, as well as risk mitigating techniques. From the regulator's viewpoint, we've a stronger appreciation of the practical challenges the industry faces. This has reinforced my belief that there continues to be a multitude of synergies that the industry and government can reap from closer collaboration and cooperation.

3 It is not by accident that we decided to call this event the "ACIP Dialogues". It represents a year of open, honest discussions between the industry and government agencies. I hope the interactions have been beneficial to everyone. We, at MAS, have been grateful to tap on the practical knowledge and expertise of all the industry representatives. For example, the trade finance training sessions conducted bythe trade-based money laundering (TBML) working group were useful refreshers on current industry practices.

4 In both working groups, there was also a concerted effort to figure out how the industry can tackle some of the emerging risks, such as those associated with the use of private investment funds, the use of similar name entities and the forgery of trade documents. I am heartened that all of us have been candid in our views, took into account various viewpoints, opposing at times, but ultimately arrived at well-thought-out solutions. The result is the best practice papers we have today. The trust we have built over the last year will be invaluable in tackling the evolving challenges we face.

Best Practice Papers

5 The two best practice papers, on TBML and misuse of legal persons, is a product of these frank conversations. The ACIP Steering Group had assessed earlier that these two areas deserve priority attention, given Singapore's status as an international trading and financial hub. Many of you here have contributed to this important work.

6 This is a fine example of co-creation and collaboration among all parties - financial institutions, audit firms, company service providers, law firms, professional advisors as well as government agencies, including CAD, Customs and MAS. David has already thanked the co-chairs of the working groups. They and their members deserve another round of thanks from me as well. Many thanks to all of you.

7 The papers contain the best practices and risk mitigation measures of industry leaders in combating TBML and the abuse of legal persons; as well as the latest "red flags" and financial crime typologies. It is relevant to financial institutions, professional services providers and other gatekeepers alike. I encourage you to study both papers, and consider how best to use the information to meet your needs. These may include incorporating the best practices into your internal policies and procedures, as well as training programmes so that your staff can better identify and mitigate the risks.

Highlights of the Best Practice Papers

8 Both papers highlight some of the latest typologies that the working group members have observed, along with established methods that criminals continue to use. Let me briefly outline a few.

9 Starting with a recurring typology, we continue to find suspicious "round-tripping" of funds through companies controlled by the same or related individuals. One example involved a network of several companies, incorporated in various jurisdictions, all with bank accounts in Singapore and controlled by the same person. The bank observed that large sums of money would flow from one company to another, before being returned within a short period of

time, under the guise of "repayment of loans". While the customer produced loan agreements to support the transactions, the customer could not explain why his companies needed to borrow from each other.

10 This case emphasises the need for banks to know your customers well, and be alert to any transactions or behaviours that are unusual or inconsistent with what you know of their business activities, source of funds and wealth, as well as their risk profile. Robust, risk-focused on-boarding and customer review practices, and well-designed screening and transaction monitoring systems, are not only fundamental, but critical defences against such threats. In fact, the company that this customer used to make the bogus loans, had a name very similar to that of a well-known company. A less astute officer might have misidentified this as a false alert. Thankfully, this was not the case here.

11 This brings me to the next, emerging typology: the use of entities with names similar to those of established or well-known companies, to make the bank believe that the entity is related to, or even the same as, the legitimate one. We have seen this across several banks, including one where a customer had a family member create companies with names identical to those of his overseas suppliers to engage in transactions with him.

12 Another recent typology is the use of "cloned" trade documents that look virtually identical to genuine ones. In one case, a Singapore company, upon receiving money from an overseas entity, remitted it to another entity in the same region. The bank found it odd that a Singapore company, despite its claim to be in the import/export business, was needed in the transaction since the trade and funds flows had no apparent link to Singapore.

13 Upon further enquiry, the company furnished invoices and shipping documents to the bank, including details to match the bill of lading to the shipping company's website. To the bank's credit, however, it didn't stop there: because the information on the website did not include details of the trading parties, the bank did a further check with the International Maritime Bureau and discovered that the names of the trading parties on the bill were forged.

14 Finally, let me touch on how private investment funds, or PIFs in short, can be abused. Private banks often endorse a set of funds, for which they provide advisory services and for which due diligence has been performed. However, their clients may also ask them to hold assets in PIFs that are separately set up by the client, which may offer trading strategies and assets that the the banks do not. For such PIFs, the full details of the funds may not be made available to the banks in order to safeguard the confidentiality of the investment strategy.

15 As you can see, this is a thorny problem: the PIF is not the bank's client, so how should the bank go about conducting due diligence and satisfy itself with the valuation and legitimacy of the PIF? I would like to commend ACIP's efforts in coming up with pragmatic solutions to address this issue. The Legal Persons Best Practice Paper highlights a number of "red flags", as well as mitigating measures centred around "knowing your security" and assessing the credibility of the valuation.

16 I could go on, but I am conscious of time and also of stealing the thunder from the panel discussions later today. Suffice to say that you can find many more notable typologies in the ACIP Best Practice Papers. With that, let me move on to the other topic I'd like to cover today: data analytics for AML/CFT.

Data Analytics

17 I am sure you would have heard MAS representatives, including myself, speak at various occasions on the importance of analytics and how excited we are about it. Allow me to share what the ACIP, as well as MAS, are doing in this area.

18 Let me start with ACIP. Over the last few months, a number of banks have started their own pilot programmes for AML/CFT analytics, covering a broad range of areas. Some of these pilots have already yielded encouraging insights and preliminary results, while others are still working through the issues. All of them have led to hard-won lessons about how to integrate data analytics tools into banks' AML/CFT controls and transactions monitoring, lessons that the broader industry could benefit from.

19 I am therefore happy to announce that ACIP member banks have come together to form a new workgroup to share their collective experience, provide practical insights on understanding, acquiring, building or co-creating AML/CFT analytics solutions. The group will also identify areas where closer collaboration between the industry and the government could lead to substantive and transformative change. I look forward to the group's findings and recommendations later in the year.

20 MAS, too, has made strides in incorporating data analytics into our supervisory work. One promising area is in STR analytics. Through the use of network analysis, we have been able to identify groups of related STRs across banks and over time among the numerous STRs that banks file every year. In some cases, there could be potential illicit activities. This is one area where banks could look into gaining deeper insights from the information you already have.

21 Another aspect is in the conduct of our inspections. Data analytics has helped us better identify problem areas, such as higher-risk accounts or transactions, for targeted reviews. This has made our inspections more focused and effective, and has yielded findings that would be more useful to the banks in enhancing their AML/CFT systems and implementation.

22 Looking ahead, MAS will be starting a series of thematic reviews, including one that focuses on the abuse of legal persons. I hope the industry takes these reviews as a learning experience: our ultimate goal is to bolster our collective AML/CFT defences, not to find fault.

23 Everyone has a part to play in combating financial crime. Through deeper collaboration between the private and public sectors, and better use of technology, we can be more effective at detecting financial crimes and mitigating such risks. Our reputation as a clean and trusted financial centre depends on our ability to protect it from abuse. As gatekeepers and service providers, your role is critical to the success of what we are seeking to achieve. Thank you and have a fruitful day ahead.