Federal Court of Australia
District Registry: New South Wales
Division: General

**CHIEF EXECUTIVE OFFICER OF THE AUSTRALIAN TRANSACTION REPORTS AND ANALYSIS CENTRE**
Applicant

**COMMONWEALTH BANK OF AUSTRALIA**
**ACN 123 123 124**
Respondent

# STATEMENT OF AGREED FACTS AND ADMISSIONS

## A INTRODUCTION

1 This Statement of Agreed Facts and Admissions (**SAFA**) is made for the purposes of s 191 of the *Evidence Act 1995* (Cth) (**Evidence Act**) jointly by the Applicant (the Chief Executive Officer (**CEO**) of the Australian Transaction Reports and Analysis Centre (**AUSTRAC**)), and the Respondent, Commonwealth Bank of Australia (**CBA**).

2 The SAFA relates to Proceedings NSD1305 of 2017 commenced by the CEO of AUSTRAC against CBA on 3 August 2017 (**Proceedings**). By the Proceedings, the CEO of AUSTRAC has sought declarations that CBA contravened particular provisions of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (**AML/CTF Act**), and orders that it pay pecuniary penalties to the Commonwealth.

3 This document identifies the facts relevant to the contraventions admitted by CBA for the purpose of the Proceedings. The facts agreed to, and the admissions made, are agreed to and made solely for the purpose of the Proceedings and do not constitute any admission outside of the Proceedings.

4 For the purposes of the Proceedings only, CBA admits that it contravened ss 36(1), 41(2)(a), 43(2) and 82(1) of the AML/CTF Act in particular respects as set out in Section D of this SAFA.

5 The parties have reached agreement as to the terms of relief to be sought from the Court to resolve the Proceedings. The parties acknowledge that, under s 175 of the AML/CTF Act, it is ultimately for the Court to determine whether CBA contravened a

civil penalty provision and the quantum of any pecuniary penalties and other relief that should be ordered.

6 The parties respectfully request that the Court make orders in the form set out in the accompanying draft orders on the basis of the specific admissions in this SAFA.

## B PARTIES AND BACKGROUND

### B.1 AUSTRAC

7 The AUSTRAC CEO is appointed pursuant to s 211 of the AML/CTF Act. She is charged with enforcing compliance with the AML/CTF Act and subordinate legislation, including the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No.1)* (**AML/CTF Rules**) and has brought the Proceedings in that capacity.

### B.2 CBA

8 CBA is a company incorporated in Australia. It is and was at all material times a reporting entity within the meaning of s 5 of the AML/CTF Act and a provider of designated services to customers within the meaning of s 6 of the AML/CTF Act.

9 At all material times, CBA has been an Authorised Deposit-Taking Institution (**ADI**), being a corporation which is authorised under the *Banking Act 1959* (Cth) (**Banking Act**) to take deposits from customers, and has been licensed to carry on banking business in Australia under the Banking Act.

10 CBA is a leading provider of financial services, including retail, business and institutional banking and wealth management products and services. It is used by as many as 1 in 3 Australians as their main financial institution.

11 CBA reported a Net Profit After Tax for the full year ending 30 June 2017 of approximately $9,928 million.[1] Of this, approximately 75% was returned to shareholders through dividends with the balance reinvested.[2]

12 CBA maintains approximately 1,350 branches, servicing approximately 16.6 million customers.[3] CBA employs approximately 51,800 people.[4]

---

[1] https://www.commbank.com.au/about-us/shareholders/financial-information/results.html (accessed 16/10/2017).

[2] CBA Annual Report 2017, page 5.

[3] CBA Annual Report 2017, page 13.

[4] CBA Annual Report 2017, page 13.

13 Reflecting its scale, size of customer base and geographic spread of operations, at all material times CBA has operated complex computer and management systems and controls. CBA processes over 16 million transactions per day.

**B.3 Background to CBA's AML/CTF operations**

14 Section 81 of the AML/CTF Act stipulates that a reporting entity must not commence to provide a designated service to a customer if the reporting entity has not adopted, and does not maintain, an anti-money laundering and counter-terrorism financing (**AML/CTF**) program, which includes a "Part A" and a "Part B".

15 Section 85(2) of the AML/CTF Act requires Part A of an AML/CTF program to:

(a) have the primary purpose of identifying, mitigating and managing the risk that the reporting entity may reasonably face that its provision of designated services might involve or facilitate money laundering or terrorism financing (**ML/TF risk**);

(b) have regard to certain matters described at Part 9.1 of the AML/CTF Rules, including the type of ML/TF risk that might be reasonably faced by the reporting entity in determining and putting in place appropriate risk-based systems and controls; and

(c) otherwise comply with the AML/CTF Rules, including by having a transaction monitoring program and an enhanced customer due diligence (**ECDD**) program that have regard to certain matters described at Chapter 15 of the AML/CTF Rules.

16 At all material times CBA has had in place:

(a) an AML/CTF function directed to the purpose of enabling CBA to comply with its obligations under the AML/CTF Act;

(b) a joint AML/CTF program which included both a Part A and a Part B (**CBA's Program**), which had been adopted by CBA; and

(c) designated management positions and personnel with direct responsibility for carrying out, and having oversight of, CBA's AML/CTF function.

17 Part A of CBA's Program was maintained and updated over time, and relevantly comprised the following versions:

(a) version 5.0 operated for the period from 28 October 2010 to 25 June 2014;

(b) version 5.5 operated for the period from 26 June 2014 to 31 December 2015;

(c) version 6.0 operated for the period from 1 January 2016 to 14 June 2016;

(d) version 7.0 operated for the period from 15 June 2016 to 5 June 2017; and

(e) version 8.0 operated for the period from 6 June 2017 to date.

18 At all material times, Part A of CBA's Program included an ongoing customer due diligence (**OCDD**) program (**OCDD Program**), which included risk-based systems and controls to monitor the provision by CBA of designated services to its customers for the purpose of identifying, mitigating and managing its ML/TF risk.

19 The OCDD Program relevantly contained:

(a) a transaction monitoring program (**Transaction Monitoring Program**), including:

(i) a Financial Crime Platform (**FCP**) operated by CBA that generated automated transaction monitoring alerts (**Automated TM Alerts**). Automated TM Alerts were triggered according to CBA's rule parameters within the FCP, which ran a system of rules over transactions in order to detect customer activity that was potentially unusual or suspicious;

(ii) a system for CBA employees who identified potentially suspicious customer activity, such as during the course of customer interactions or periodic review of customer transaction data, to raise manual alerts (**Manual Alerts**), generally by completing a Suspect Transaction Report (**STR**);

(iii) a platform for receiving and reviewing both Automated TM Alerts and Manual Alerts and filing suspicious matter reports (**SMRs**), being the Pegasus Financial Crime Case Management System (**Pegasus**);

(b) a system for complying with CBA's suspicious matter reporting obligations; and

(c) an enhanced customer due diligence (**ECDD**) program (**ECDD Program**), including risk-based systems and controls directed to undertaking measures appropriate to the circumstances in cases where one or more of the circumstances in r 15.9 of the AML/CTF Rules arises.

20 Underpinning CBA's Program, at all material times, CBA had in place a number of further documents including Group Standards, Standard Operating Procedures, User Guides and Reference Guides, which were maintained by CBA and updated from time to time. These documents provided further specificity of the requirements, processes, systems and controls for CBA's Program, including in respect of the OCDD Program and CBA's approach to ML/TF risk.

21 In support of the OCDD Program, at all material times CBA employed a team of personnel who were responsible for reviewing and investigating Automated TM Alerts and Manual Alerts, considering and actioning SMRs and undertaking ECDD as required (**AML Operations team**). Responsibilities within the AML Operations team were further divided into groups that included a Transaction Monitoring team and a Customer Risk team. During the relevant period, within these groups:

(a) Analysts in the Transaction Monitoring team were responsible for the initial review and investigation of Automated TM Alerts and Manual Alerts, related customer due diligence and escalation of potentially suspicious matters to Senior Analysts within the same team;

(b) Senior Analysts in the Transaction Monitoring team were responsible for considering escalated matters, forming suspicions and submitting SMRs to the AUSTRAC CEO where appropriate, and performing quality assurance on the work undertaken by Analysts;

(c) Analysts in the Customer Risk team were responsible for the initial review and investigation of High Risk Customer (**HRC**) alerts, considering customers who had been subject to SMRs and designating customers with HRC status, undertaking further customer due diligence in respect of HRC customers and customers who had been subject to SMRs and PEPs, and preparing HRC reports recommending to the relevant business unit whether to terminate a business relationship with a customer; and

(d) Senior Analysts in the Customer Risk team were responsible for reviewing and approving HRC reports and other matters escalated by Analysts, escalating HRC reports to relevant business units once approved and performing a second level review and quality assurance on the work undertaken by Analysts.

## C FACTS RELEVANT TO LIABILITY

### C.1 Risk Assessments

22 By section 82(1) of the AML/CTF Act, CBA was obliged to comply with Part A of CBA's Program.

23 As required by the AML/CTF Act and AML/CTF Rules, at all material times Part A of CBA's Program (and documents underpinning this, including a Group Standard on Risk Identification and Assessment Methodology) required that CBA identify, mitigate and manage ML/TF risk by undertaking ML/TF risk assessments, including in respect of new methods of designated service delivery and new or developing technologies used for the provision of a designated service prior to adopting them.

24 CBA's Program, under Part A and the applicable Group Standard, required it to:

(a) assess the inherent ML/TF risk posed by each new method of designated service delivery and new or developing technology prior to adoption;

(b) review ML/TF risk assessments where there are significant instances of money laundering using CBA's products or services;

(c) carry out periodic reviews of risk attributes and methodologies; and

(d) ensure any material ML/TF risks identified were to be subject to systems and controls to manage them.

25 Risk assessments are a central component of a reporting entity's compliance with the obligation to mitigate and manage ML/TF risk.

26 In May 2012, CBA introduced a new channel for providing designated services in the form of an Intelligent Deposit Machine (**IDM**). IDMs were introduced as part of a project to refresh CBA's Automated Teller Machine (**ATM**) fleet, starting with 5 IDMs. The IDM was, and is, a type of ATM which has the functionality to accept cash and cheque deposits into CBA accounts. Funds could be deposited using a CBA branded card or a card of any other financial institution (**OFI**). Funds can only be deposited to the account of a CBA customer. In contrast to an ordinary or older ATM, any cash deposited through an IDM is automatically counted by the machine and is instantly credited to the nominated beneficiary CBA account. Those funds are immediately available for transfer, including for international transfer. In November 2017, a daily limit was applied to cash deposits made to a CBA customer's personal account when the cash was deposited using a CBA branded card. In April 2018, daily limits were implemented on the amount of cash that could be deposited into a CBA customer's personal or business account via an IDM.

27 The ML/TF risks of providing designated services through IDMs were high and obvious at all relevant times because cash could be deposited anonymously at any time at hundreds of locations and transferred immediately, either domestically or internationally, without any limit being imposed.

28 Prior to the introduction of IDMs, CBA considered certain AML/CTF matters, including identifying that threshold transactions might occur through IDMs and designing systems to notify those transactions to AUSTRAC through threshold transaction reports (**TTRs**). At all times from the launch of IDMs, CBA applied its Transaction Monitoring Program to transactions occurring through IDMs. However, contrary to the requirements of CBA's Program, CBA did not undertake an ML/TF risk assessment specific to IDMs prior to them being introduced.

29 The ML/TF risks of IDMs changed significantly throughout the period on and from May 2012 when IDMs were first rolled out, as cash deposits into IDMs grew. In May 2012

when the first 5 IDMs were first rolled out, cash deposits for that month totalled $868,825. By May 2017, at which time there were 805 IDMs, cash deposits for that month were about $1.7 billion.

30 In 2014, CBA submitted SMRs to AUSTRAC relating to suspicions that money-laundering was occurring through its IDMs. However, CBA did not at that time undertake an ML/TF risk assessment of its IDMs and no new and appropriate risk-based controls were introduced to mitigate and manage the high ML/TF risks of IDMs.

31 By around July 2015, CBA had evidence that criminal syndicates were laundering several millions of dollars through its IDMs. CBA identified these significant instances of money laundering through its own transaction monitoring and its own intelligence and analysis, and was interacting with law enforcement regarding this activity, including with serious organised crime units of the Australian Federal Police (**AFP**). CBA later also interacted with New South Wales Police and Western Australian Police regarding this activity.

32 In July 2015, CBA undertook an assessment of the inherent ML/TF risk of IDMs and assessed the IDMs to have a high inherent ML/TF risk. However, this assessment did not follow the procedures set out in CBA's Program and no new and appropriate risk-based controls were introduced to mitigate and manage the high ML/TF risks of IDMs.

33 On 18 December 2015, AUSTRAC provided a number of banks, including CBA, with a confidential Methodologies Brief regarding ATM Deposits (the **Methodologies Brief**). In the Methodologies Brief, AUSTRAC identified possible indicators to assist industry to identify potential money laundering through ATMs (with the reference to ATMs being understood to include reference to IDMs). The Methodologies Brief recorded that ATMs presented money laundering syndicates with the opportunity to deposit large amounts of cash into accounts without imposing a daily cash deposit limit. This lack of daily deposit limits, coupled with the ability to deposit cash anonymously, was said to present a 'significant vulnerability'.

34 However, CBA did not at that time undertake an ML/TF risk assessment of its IDMs and no new and appropriate risk-based controls were introduced to mitigate and manage the high ML/TF risks of IDMs. CBA did not act at that time to introduce daily limits for cash deposits through IDMs to mitigate or manage the identified risk. CBA continued to rely on detective controls in the form of its Transaction Monitoring Program, but acknowledges that these controls were not appropriately risk-based.

35 In July 2016, CBA undertook a further assessment of the inherent ML/TF risk for IDMs. CBA again assessed the IDMs to have a high inherent ML/TF risk, but concluded that the residual risk of the IDMs were low, taking into account application of CBA's Transaction Monitoring Program. The risk assessment noted that SMRs were being submitted in respect of transactions conducted through IDMs and so were

successfully identifying suspicious transactions. However, this assessment did not follow the procedures set out in the CBA's Program and no new and appropriate risk-based controls were introduced to mitigate and manage the high ML/TF risks of IDMs.

36 CBA undertook a further assessment of the inherent ML/TF risk for IDMs in October 2017, after the commencement of these proceedings. CBA decided to impose daily limits to cash deposits through IDMs. In that risk assessment, CBA recorded its decision to introduce daily limits for cash deposits made using personal CBA branded cards, business CBA branded cards and OFI cards. This was to be done in stages (due to time needed to effect the change in systems). In November 2017, CBA imposed daily limits on cash deposits through IDMs in the form of a $20,000 limit on cash deposits made to personal CBA accounts using a CBA branded card. No daily limits were introduced for cash deposits into CBA accounts using OFI cards. No limits were imposed on the number of CBA branded cards that could be used to deposit cash daily into CBA accounts. No daily limits were introduced for deposits, using a CBA branded card, into CBA business accounts. There were no daily limits on the amount of cash that could be deposited into a CBA account.

37 In April 2018, CBA undertook a further assessment of the inherent ML/TF risk for IDMs. CBA decided to impose a $10,000 limit on cash deposits through IDMs made to CBA personal and business accounts, subject to accounts of certain business customers and institutional banking customers having a higher limit. On 12 April 2018, CBA implemented those account-based daily limits.

38 It was not until CBA introduced daily limits on cash deposits through IDMs commencing in November 2017 and completed by 12 April 2018 that CBA adopted sufficient appropriate risk-based controls to mitigate and manage the ML/TF risk posed by IDMs.

39 As a consequence of the matters set out in paragraphs 28 to 38 above, CBA contravened s 82(1) of the AML/CTF Act on 14 occasions by failing to comply with procedures in its Part A Program by failing to:

(a) undertake an assessment of the inherent ML/TF risk in respect of IDMs prior to the introduction of IDMs in or around May 2012;

(b) introduce sufficient appropriate risk-based controls to mitigate and manage the ML/TF risks posed by IDMs in or around May 2012;

(c) undertake a periodic assessment of the inherent ML/TF risk in respect of IDMs in early 2014;

(d) introduce sufficient appropriate risk-based controls to mitigate and manage the ML/TF risks posed by IDMs by introducing daily limits in early 2014, following the periodic assessment;

(e) undertake an assessment of the inherent ML/TF risk in respect of IDMs in mid to late 2014;

(f) introduce sufficient appropriate risk-based controls to mitigate and manage the ML/TF risks posed by IDMs by introducing daily limits in mid to late 2014;

(g) undertake an assessment of the inherent ML/TF risk in respect of the IDMs that complied with CBA's Program in July 2015;

(h) introduce sufficient appropriate risk-based controls to mitigate and manage the ML/TF risks posed by IDMs by introducing daily limits in July 2015;

(i) undertake an assessment of the inherent ML/TF risk in respect of the IDMs in December 2015;

(j) introduce sufficient appropriate risk-based controls to mitigate and manage the ML/TF risks posed by IDMs by introducing daily limits in December 2015;

(k) undertake a periodic assessment of the inherent ML/TF risk in respect of IDMs that complied with CBA's Program in mid-2016;

(l) introduce sufficient appropriate risk-based controls to mitigate and manage the ML/TF risks posed by IDMs by introducing daily limits in mid-2016, following the periodic assessment;

(m) undertake an assessment of the inherent ML/TF risk in respect of the IDMs that complied with CBA's Program in 2017 at a time prior to October 2017; and

(n) introduce sufficient appropriate risk-based controls to mitigate and manage these ML/TF risks by introducing daily limits in 2017 at a time prior to November 2017.

**C.2 Threshold Transaction Reporting to AUSTRAC**

40 By s 43(2) of the AML/CTF Act, CBA was at all material times obliged to submit a TTR to the AUSTRAC CEO within 10 business days after the day on which a threshold transaction took place.

41 Between November 2012 and September 2015, CBA failed to submit TTRs in respect of 53,506 threshold transactions to the AUSTRAC CEO within 10 business days after the day on which the transaction took place.

42 The 53,506 TTRs relate to certain cash deposits which occurred through IDMs. Between May 2012 and October 2012, CBA had in place an automated process to identify threshold transactions through IDMs and report TTRs to the AUSTRAC CEO (the **TTR process**). The TTR process identified transactions by transaction codes and

automatically generated TTRs in respect of threshold transactions by reference to those transaction codes.

43 When IDMs were launched, two transaction codes were used to identify the types of deposits involving cash that could be made through IDMs, being transaction codes 5022 and 4013. CBA's system for TTR reporting was programmed to identify cash transactions of $10,000 or more deposited via an IDM by undertaking an automated search of system data for transactions using these transaction codes. Where the amount of cash deposited (or the cash component where it was a mixed deposit of cash and cheque) was $10,000 or more, the system automatically generated a TTR for submission to AUSTRAC.

44 In June 2012, an issue was identified regarding an error message which appeared in Netbank, CBA's electronic banking site for its customers, in respect of cash-only deposits made at IDMs. In or around November 2012, to address that error message appearing in Netbank, a third transaction code was introduced for certain cash deposits through IDMs, being transaction code 5000. However, at that time the TTR process was inadvertently not updated and configured to automatically search for transactions with the transaction code 5000 (in addition to the 5022 and 4013 transaction codes) for the purposes of TTR reporting to AUSTRAC. As a result, cash deposits through IDMs identified by transaction code 5000 did not automatically generate TTRs from 5 November 2012 to 1 September 2015. Each of the 53,506 TTRs was a cash deposit through an IDM which was identified by reference to transaction code 5000.

45 On 11 August 2015, AUSTRAC contacted CBA regarding two threshold transactions made through IDMs that were referred to in an SMR submitted by CBA to the AUSTRAC CEO on 7 August 2015, in circumstances where AUSTRAC could not find two corresponding TTRs being given by CBA. In investigating this inquiry, CBA identified that TTRs were potentially not being reported automatically in the case of threshold transactions involving certain cash deposits through IDMs.

46 As described further at paragraph 70 below, CBA immediately took steps to investigate and address this issue, in the course of which it identified the 53,506 threshold transactions in respect of which TTRs had not been submitted.

47 CBA ultimately submitted 2 of the TTRs to the AUSTRAC CEO late on 24 August 2015 and the remaining 53,504 TTRs late on 24 September 2015.

48 As a consequence of the matters set out in paragraphs 41 to 47 above, CBA contravened s 43(2) of the AML/CTF Act by failing to give 53,506 TTRs to the AUSTRAC CEO within the timeframe stipulated by s 43(2) of the AML/CTF Act.

### C.3 Transaction Monitoring Program

49 By section 82(1) of the AML/CTF Act, CBA was obliged to comply with Part A of CBA's Program.

50 At all relevant times, Part A of CBA's Program provided that certain CBA products and services were to be subject to 'Priority Monitoring'. The expression 'Priority Monitoring' relevantly referred to the automated monitoring of transactions conducted through those products and services (including account-level monitoring) using a systems-based solution. The FCP was one such systems-based solution.

51 From 20 October 2012 to 12 October 2015, Automated TM Alerts were not always generated as intended, either at all or for a period of time, in respect of 778,370 accounts (together, the **Affected Accounts**), which accounts were otherwise intended to be subject to account-level automated transaction monitoring through the FCP. This occurred as a result of an error, which arose in the process of merging data from two systems on or around 20 October 2012. Due to the error:

(a) the 'account type description' field (which indicated whether the account was a personal account or a commercial account) for each of the Affected Accounts was not populated within the FCP; and

(b) as a result, the account-level automated transaction monitoring rules did not operate as intended in respect of the Affected Accounts, in circumstances where automated transaction monitoring rules depended on whether an account was described as either a personal account or a commercial account.

52 CBA identified the computer coding error itself on or around 16 June 2014. By or about 19 September 2014, it had undertaken rectification work such that the error was fixed and could no longer cause the 'account type description' field of CBA accounts to be left blank. By 12 October 2015:

(a) CBA had completed the population of the 'account type description' field for each of the Affected Accounts; and

(b) automated transaction monitoring was operating as intended in respect of the Affected Accounts, which were each subject to account-level automated transaction monitoring.

53 As a consequence of the matters set out in paragraphs 50 to 52 above, CBA failed to comply with its Transaction Monitoring Program in respect of the Affected Accounts, in contravention of s 82(1) of the AML/CTF Act, from 20 October 2012 to 12 October 2015.

### C.4 Suspicious matter reporting to AUSTRAC

54 By s 41(2)(a) of the AML/CTF Act, CBA was at all material times obliged to submit an SMR to AUSTRAC within 3 business days of forming a suspicion on reasonable grounds that either:

(a) a person to whom it commenced, or proposed, to provide a designated service was not the person they claimed to be; or

(b) CBA had information concerning the provision, or prospective provision, of that designated service that may be relevant to the investigation of, or prosecution of a person for, an offence against a law of the Commonwealth or of a State or Territory.

55 Between 28 August 2012 and 7 June 2017, CBA did not submit SMRs to AUSTRAC within the time frame stipulated by s 41(2)(a) as follows:

(a) On 40 occasions, CBA did not submit SMRs, within the required time frame, in relation to instances of suspicious account activity indicative of possible money laundering or structuring transactions to evade TTR requirements, in circumstances where CBA had already submitted an SMR in relation to the relevant customer within the previous 3 months about a similar pattern of activity on the same account. In 18 of these cases, CBA did not submit SMRs to AUSTRAC within the time frame stipulated in s 41(2)(a) although it subsequently did so. In the remaining 22 cases, CBA did not submit SMRs to AUSTRAC at all.

This approach was adopted by the Transaction Monitoring team due to a misapprehension of the requirements of s 41 of the AML/CTF Act. CBA accepts that it ought to have submitted SMRs on each occasion when further suspicious transactions were identified regardless of whether they were considered to be qualitatively similar.

(b) On 69 occasions, CBA did not submit SMRs, within the required time frame, in relation to instances of suspicious account activity indicative of possible money laundering, dealing in proceeds of crime or otherwise understood to be relevant to a criminal investigation, in circumstances where CBA had received requests from law enforcement for account details in the context of a criminal investigation. In 50 of these cases, CBA did not submit SMRs to AUSTRAC within the time frame stipulated in s 41(2)(a) although it subsequently did so. In the remaining 19 cases, CBA did not submit SMRs to AUSTRAC at all. This was due to a misapprehension about the proper treatment of information received from law enforcement. Further, of these occasions:

(i) 7 of the cases relate to customers the subject of an AFP investigation into a possible money laundering syndicate (**Syndicate 1**);

(ii) 6 of the cases relate to customers the subject of a New South Wales Police investigation into a possible cuckoo smurfing syndicate (**Strike Force A1**), with each customer being listed in the same email notification to CBA from the New South Wales Police;

(iii) 6 of the cases relate to customers the subject of a New South Wales Police investigation into a possible cuckoo smurfing syndicate (**Strike Force A2**), with each customer being listed in the same email notifications to CBA from the New South Wales Police;

(iv) 2 of the cases relate to customers the subject of a WA Police investigation into a possible money laundering syndicate (**WA Police Operation**);

(v) 3 of the cases relate to customers the subject of an AFP investigation into a possible money laundering syndicate (**Syndicate 4**);

(vi) 1 case relates to a customer the subject of an AFP investigation into a separate possible criminal syndicate (**Syndicate 2**); and

(vii) the remaining 44 cases relate to customers the subject of a New South Wales Police investigation into a further separate possible criminal syndicate (**Strike Force B**), with each customer being listed in the same two notifications to CBA from the New South Wales Police.

(c) On 29 occasions, CBA did not submit SMRs, within the required time frame, in relation to suspicions that account holders were not the people they claimed to be, in circumstances where 29 accounts were opened by two individuals within a criminal syndicate (**Syndicate 1**) using false identification, and where CBA had received information from law enforcement to this effect with the customers being listed across two email notifications to CBA from the AFP. This was due to a misapprehension that information of this nature derived from law enforcement did not need to be reported to AUSTRAC. CBA accepts that it ought to have submitted SMRs in respect of this information and that, although it subsequently reported the information, it did not do so within the time required by the AML/CTF Act.

(d) On 11 occasions, CBA did not submit SMRs, within the required time frame, in relation to instances of suspicious account activity indicative of possible

money laundering, dealing in proceeds of crime or structuring transactions to evade TTR requirements, in circumstances of discrete error. In 1 of these cases, CBA reported the transactional activity in an SMR 3 weeks late. In the remaining 10 cases, CBA did not submit SMRs to AUSTRAC at all.

56 As a consequence of the matters set out in paragraph 55 above, CBA contravened s 41(2)(a) of the AML/CTF Act on each occasion.

**C.5 Customer Due Diligence**

57 By s 36(1) of the AML/CTF Act, CBA was obliged to monitor its customers with a view to identifying, mitigating and managing the risk it reasonably faced that the provision of a designated service might (whether inadvertently or otherwise) involve or facilitate money laundering or terrorism financing, and to do so in accordance with the AML/CTF Rules.

58 Between 15 December 2011 and 1 February 2018, CBA did not comply with its obligations under s 36(1), either at all or for a specified period of time, in respect of 80 customers, which failure to comply came about where:

(a) insufficient Automated TM Alerts were generated on the customer's account for a period in circumstances where there were transactions that were complex, unusually large, had an unusual pattern, or which had no apparent economic or visible lawful purpose. In most of these cases the affected period ranged from 2 weeks to 18 months, but in some cases the affected period exceeded 2 years;

(b) alerts had been generated in respect of the customer or account, but a review of the customer or account did not occur quickly enough once that alert had been triggered. In most cases the affected period was 2 months or less, but in one case the affected period was 18 months;

(c) insufficient consideration was given as to whether CBA should terminate the customer relationship having regard to the ML/TF risk posed by the customer. In most of these cases the affected period ranged between 1 and 8 months, but in one case the affected period was 19 months;

(d) 30 days' notice was provided to customers of CBA's intention to terminate the customer relationship and close the account, during which the customers were able to continue transacting without heightened restrictions in place. The delay in rendering the account inactive once the decision to terminate had been made resulted in further suspicious or unusual transactional activity;

(e) it otherwise did not undertake enhanced customer due diligence measures appropriate to the circumstances to mitigate or manage its ML/TF risk in respect of the customer in accordance with the AML/CTF Rules; or

(f) a combination of the above factors occurred.

59 As a consequence of the matters set out in paragraph 58 above, CBA contravened s 36(1) of the AML/CTF Act on each occasion.

## D FORMAL ADMISSIONS

60 By reason of the matters set out above, CBA makes the following admissions for the purpose of the Proceedings:

(a) CBA contravened s 82(1) of the AML/CTF Act on 14 occasions as identified in paragraph 39.

(b) CBA contravened s 43(2) of the AML/CTF Act on 53,506 occasions by failing to give TTRs to the AUSTRAC CEO within the time frame stipulated by s 43(2) of the AML/CTF Act as identified in paragraphs 41 to 48 of the SAFA.

(c) CBA contravened s 82(1) of the AML/CTF Act from 20 October 2012 to 12 October 2015, by failing to comply with provisions of Part A of its Program relating to transaction monitoring in respect of the Affected Accounts as identified in paragraphs 49 to 53 of the SAFA.

(d) CBA engaged in contraventions of s 41(2)(a) of the AML/CTF Act between 28 August 2012 and 7 June 2017 by failing to submit an SMR to AUSTRAC, either within the time frame stipulated in s 41(2)(a) or in some instances at all, on 149 occasions as identified in paragraphs 55 to 56 of the SAFA.

(e) CBA engaged in 80 contraventions of s 36(1) of the AML/CTF Act between 15 December 2011 and 1 February 2018 by failing to monitor customers with a view to identifying, mitigating and managing ML/TF risks, as identified in paragraphs 58 to 59 of the SAFA.

## E FACTS RELEVANT TO RELIEF

### E.1 Nature and extent of the contraventions

**Risk Assessments**

61 CBA's admitted contraventions in respect of its failures to comply with CBA's Program in not undertaking ML/TF risk assessments for IDMs either at all or that complied with CBA's Program prior to October 2017 carries a maximum penalty of up to $21 million each. CBA's admitted contraventions in respect of its failures to introduce sufficient appropriate risk-based systems and controls in respect of IDMs by not introducing

daily limits until it commenced introducing daily limits in November 2017 and completed doing so in April 2018 carries a maximum penalty of up to $21 million each.

62 None of the contraventions was the result of any deliberate intention to breach the AML/CTF legislation.

63 However, these contraventions are serious for the following reasons:

(a) The requirement to undertake an ML/TF risk assessment of a new channel is a central aspect of the AML/CTF regulatory regime, as well as being a key element of CBA's Program. It provides an appropriate means for ensuring that the reporting entity is in a position to identify, mitigate and manage its ML/TF risk.

(b) The IDMs posed a high ML/TF risk because cash could be deposited anonymously at any time at hundreds of locations and transferred immediately, either domestically or internationally, without any limit being imposed.

(c) CBA failed to undertake an ML/TF risk assessment of its IDM channel that complied with its Program for a period of 6 years. During that time, CBA's IDM fleet grew significantly from 5 to 1,118 machines. As the number of IDMs grew, there was also an exponential increase in cash deposited through IDMs. Between June and November 2012, approximately $89 million of cash was deposited through IDMs (the number of IDMs had increased from 5 to 58). Between January and June 2016, approximately $5.81 billion of cash was deposited through IDMs (the number of IDMs had increased from 602 to 711). By May 2017, by which time there were 805 IDMs, monthly cash deposits were about $1.7 billion.

(d) In and from March 2014, CBA submitted SMRs to AUSTRAC related to suspicions that money-laundering was occurring through its IDMs. By around July 2015, CBA had evidence that criminal syndicates were laundering money using its IDMs and was interacting with law enforcement regarding this activity, including with the serious organised crime units of the Australian Federal Police. CBA later also interacted with the New South Wales Police and Western Australian Police regarding this activity.

(e) When CBA did undertake an assessment of the inherent ML/TF risk of IDMs in July 2015, the risk assessment did not comply with CBA's Program and nor did it introduce daily limits at that time.

(f) CBA did not to take steps responsive to AUSTRAC's Methodologies Brief of December 2015 in which the high ML/TF risks of IDMs were set out.

(g) As the high inherent risks of IDMs were known to CBA, it was particularly important for there to be a thorough assessment of the risks in accordance with the procedures set out in CBA's Program and for appropriate risk-based systems and controls to be put in place for mitigating and managing that risk.

(h) When CBA did undertake an assessment of the inherent ML/TF risk of IDMs in July 2016, the risk assessment did not comply with CBA's Program and CBA did not introduce daily limits at that time.

(i) While transactions through IDMs were at all times subject to automated transaction monitoring as a detective control, based on the information available to CBA as described in paragraphs 30, 31 and 33 above, CBA ought to have introduced daily limits on cash deposits through IDMs as a control for mitigating and managing its ML/TF risk and yet it did not implement daily limits on cash deposits through IDMs into CBA accounts until it commenced doing so in November 2017 and completed doing so in April 2018.

(j) During the time that daily limits had not been introduced, several million dollars of money-laundering occurred through CBA's IDMs and some of the persons involved in the syndicates laundering money through IDMs have been prosecuted and convicted of unlawful activity.

(k) Had CBA introduced daily limits earlier it would have disrupted money laundering activity through IDMs by syndicates involved in the importation and distribution of drugs including methamphetamine.

64 The contraventions also came about in circumstances where:

(a) CBA had procedures requiring that an ML/TF risk assessment be undertaken on the introduction of a new channel, and a system directed to achieving this, as reflected in both Part A and a specific Group Standard directed to ML/TF risk assessments. The Group Standard contained templates for ML/TF risk assessments to be used by the Business units. CBA failed to follow these procedures on numerous occasions.

(b) At the time the IDMs were launched, CBA had undertaken an ATM ML/TF risk assessment and had dedicated AML & Sanctions personnel who were responsible for undertaking ML/TF risk assessments. However, the ML/TF risks of IDMs were different and significantly and obviously higher than the ML/TF risks of ATMs.

(c) Personnel with responsibility for preparing ML/TF risk assessments were involved in the project to introduce IDMs. Prior to launch, they considered AML/CTF matters in respect of the IDMs as discussed in paragraph 28

above, including to set up a process to automatically report TTRs to AUSTRAC. However, CBA overlooked the fact that no ML/TF risk assessment specific to IDMs had been completed prior to launch of the IDMs.

(d) During the period of the contraventions, CBA introduced improvements to its ML/TF risk assessment process, including updating the Group Standard 'Global Financial Crime Risk Identification and Assessment Methodology' in July 2016, and again in December 2016 and December 2017, and creating a risk assessment tool to better equip the Business units to complete ML/TF risk assessments as required by CBA's Program and Group Standard.

(e) At all material times, transactions made through IDMs were subject to CBA's Transaction Monitoring Program, although alerts were not always raised or reviewed in a timely manner as described in Section C.5 above, and daily limits as an appropriate risk-based preventative control were implemented commencing in November 2017 and completed in April 2018.

65 Since the time of these contraventions, CBA has undertaken a range of further enhancements in respect of risk assessments, as set out in paragraphs 116 and 117 below.

**Threshold Transaction Reporting to AUSTRAC**

66 CBA's admitted failure to give 53,506 TTRs to the AUSTRAC CEO within the time frame specified by s 43(2) of the AML/CTF Act occurred in the circumstances described in paragraphs 41 to 47 above. At the time the non-compliance commenced in November 2012, a contravention carried a maximum penalty of $11 million. Over the period when TTRs were not given to AUSTRAC within the statutory time frame, the maximum pecuniary penalty for a body corporate under the AML/CTF Act ranged between $11 million and $18 million for each contravention. For the majority of the relevant period, the penalty was $17 million for each contravention.

67 None of the contraventions was the result of a deliberate intention to breach the AML/CTF legislation.

68 The contraventions were serious because:

(a) they were caused by a lack of risk management, assurance and oversight that endured for close to 3 years. The contraventions were not identified until AUSTRAC drew reporting anomalies to CBA's attention;

(b) TTRs provide valuable information to AUSTRAC and the law enforcement agencies that access that information from AUSTRAC. The value of a TTR diminishes substantially if it is not lodged on time, as funds can no longer be traced and ongoing activity cannot be promptly identified and monitored;

(c) while CBA did ultimately submit all required TTRs to AUSTRAC by 24 September 2015, the failure of CBA to give TTRs to AUSTRAC within the requisite time frame impeded the efforts of AUSTRAC and law enforcement agencies by depriving them of intelligence that the AML/CTF Act intends they be supplied; and

(d) the late TTRs numbered 53,506 and represented about 95% of threshold transactions that occurred through IDMs in the relevant period and had a total value of $624.7 million. 1,656 of the late TTRs (totalling about $17.5 million) related to transactions connected with money laundering syndicates being investigated and prosecuted by the AFP or accounts connected with those investigations. A further 6 of the late TTRs related to 5 customers who had been assessed by CBA as posing a potential risk of terrorism or terrorism financing.

69 The contraventions also came about in the following circumstances:

(a) CBA had established a TTR process to automatically identify and report to AUSTRAC threshold transactions occurring through IDMs, which process had been tested at its launch to confirm that it was working as intended.

(b) The automated TTR process did not operate as it was intended to do in respect of the 53,506 admitted late TTRs following the coding error described in paragraphs 42 to 44 above and occurring after launch.

(c) Although this led to TTRs being submitted late, CBA did take steps during the relevant period to identify, mitigate and manage ML/TF risk in respect of the affected customers, and provide other intelligence to AUSTRAC and law enforcement, by the broader application of its Transaction Monitoring Program.

(d) The application of the Transaction Monitoring Program led to CBA considering Automated TM Alerts and Manual Alerts and submitting SMRs to AUSTRAC in respect of transactional activity through IDMs, including as relating to customers the subject of one or more late TTRs. However, the full scale of the suspicious cash activity through IDMs was not reported to AUSTRAC, as set out in Sections C.4 and C.5 above.

(e) The 53,506 TTRs given by 24 September 2015 represented 2.3% of the total TTRs given by CBA to AUSTRAC in the period from November 2012 to September 2015, which totalled approximately 2.3 million TTRs.

70 Following the identification of the issue, CBA immediately took steps to investigate and address this issue. This involved CBA:

(a) identifying the root cause of the error and implementing a fix for the error, which involved configuring the TTR process to automatically search system data for threshold transactions using transaction code 5000 for the purpose of those transactions automatically being reported to AUSTRAC as TTRs;

(b) disclosing the issue to AUSTRAC on 8 September 2015; and

(c) identifying all cash deposits of $10,000 or more made through IDMs that had the transaction code 5000 and in respect of which a TTR had not been given to AUSTRAC and filing TTRs by 24 September 2015.

71 Since the time of these contraventions, CBA has undertaken a range of further enhancements in respect of TTRs, as set out in paragraphs 118 and 119 below.

**Transaction Monitoring Program**

72 CBA has admitted that it contravened s 82(1) of the AML/CTF Act from 20 October 2012 to 12 October 2015. During this period, the maximum penalty for a contravention of s 82(1) was between $11 million and $18 million, but for the majority of the period the maximum penalty was $17 million for each contravention.

73 None of the contraventions was the result of a deliberate intention to breach the AML/CTF legislation.

74 The effect of the error referred to in paragraph 51 above on CBA's automated transaction monitoring system was not identified during the contravening period. However, more should have been done to investigate its impact on its transaction monitoring of the Affected Accounts and fix the issue sooner than was done.

75 The number of unmonitored transactions that occurred on the Affected Accounts during the contravening period is unknown. The precise number of contraventions therefore cannot be ascertained, but is potentially very significant. As set out in paragraph 51 above, this stemmed from the same error, which occurred on or around 20 October 2012.

76 The error was not known to CBA at the time it occurred, and was only identified by CBA on or around 16 June 2014, due to a lack of assurance processes. As set out in paragraph 52 above, CBA rectified the computer coding error on or about 19 September 2014, but did not ensure that the Affected Accounts were each subject to account level automated transaction monitoring until 12 October 2015.

77 The contraventions are serious for the following reasons:

(a) For a period of just under 3 years, CBA was not undertaking the intended level of transaction monitoring on the Affected Accounts, having regard to the need to identify, mitigate and manage its ML/TF risk, as reflected in its Transaction Monitoring Program. This could have impeded the efforts of

AUSTRAC and law enforcement agencies by depriving them of intelligence that the AML/CTF Act intends they be supplied. With transaction monitoring not operating as intended either at all or for some of this period on the Affected Accounts, there was very little scope to identify, having regard to ML/TF risk, any transaction that appeared to be suspicious within the terms of s 41 of the Act at those times.

(b) CBA failed to promptly detect that automated transaction monitoring was not operating as intended.

(c) There were not adequate systems and controls to prevent an issue of this kind from affecting the operation of CBA's Transaction Monitoring Program, and to detect and respond to it quickly.

(d) CBA correctly assesses bank accounts, as a product, to be high risk. All CBA accounts should have been subject to transaction monitoring proportionate to this risk.

78 The contraventions occurred in the following circumstances:

(a) CBA had a Transaction Monitoring Program.

(b) The Transaction Monitoring Program was supported by processes and systems (including the FCP) designed to enable CBA to monitor transactions across CBA accounts, including the Affected Accounts. The FCP was, and continues to be, a large-scale and significant platform by which CBA conducted daily monitoring of the transactions of its customers.

(c) The issue arose as a result of an unintentional coding error which occurred in the process of merging data from two systems as described above.

(d) CBA itself detected the issue and took steps to resolve the issue.

79 Since the time of contraventions, CBA has undertaken a range of further enhancements in respect of the matters the subject of these contraventions, as set out in paragraph 120 below.

**Suspicious matter reporting to AUSTRAC**

80 CBA's admitted contraventions in respect of failures to file SMRs (either on time or, in some instances, at all) occurred in the period from 28 August 2012 (at which point the maximum penalty was $11 million for each contravention) to 7 June 2017 (at which point the maximum penalty was $18 million for each contravention). The majority of these contraventions occurred between March 2015 and December 2015, with the maximum penalty in December 2015 being $18 million for each contravention.

81 None of the admitted contraventions was the result of a deliberate intention to breach the AML/CTF legislation. However, CBA did make a deliberate decision to implement the '3 month policy' on the misunderstanding that this approach was compliant.

82 The contraventions were serious because:

(a) CBA repeatedly failed to report obvious and very specific patterns of structuring indicative of money laundering, including through IDMs, despite having identified it, thereby failing to comply with its obligations to give an SMR to AUSTRAC either at all or within the time required by s 41 of the Act. In part, this was because CBA adopted a policy not to submit SMRs if the same type of suspicious behaviour had been reported any time within the previous 3 months. CBA also failed to lodge SMRs because notifications by law enforcement of unlawful activity on specific accounts were not appropriately actioned.

(b) CBA also failed to report suspicions in relation to identity fraud.

(c) The reporting failures concerned 8 money laundering syndicates and 1 suspected unregistered remittance dealer.

(d) Whilst the matters at paragraphs 55(a) to (c) above were due to a misapprehension of the requirements of s 41 of the AML/CTF Act, CBA is a large and well-resourced entity that should understand its obligations under the AML/CTF Act, especially in circumstances where it was dealing with officers from the serious organised crime units of law enforcement who were providing the bank with detailed information.

(e) AUSTRAC and law enforcement were denied intelligence to which they are entitled under the Act involving several million dollars of proceeds of crime – mostly connected with drug importation and distribution, which intelligence could have been used to identify, disrupt and prosecute this unlawful activity.

83 The contraventions came about in circumstances where:

(a) at all material times:

(i) CBA's Program was in place, which included a system for complying with CBA's SMR obligations as referred to in paragraph 19(b) above.

(ii) CBA's approach to its SMR obligations, as described in CBA's Program, was supported by a range of Group Standards, Standard Operating Procedures, User Guides and Reference Guides.

(iii) CBA had a Transaction Monitoring team whose day to day responsibilities included considering Automated TM Alerts and

Manual Alerts (and related investigations) for the purpose of detecting suspicious activity and ensuring that CBA met its SMR obligations, as referred to in paragraph 21 above. The Transaction Monitoring team carried out its functions from a centralised operations centre and the team was subject to oversight by Managers and an Executive Manager within that team.

(iv) The Transaction Monitoring team received both formal and informal training in respect of the discharge of CBA's SMR obligations, including as detailed in paragraph 121(c) below.

(b) during the period of the contraventions, CBA made a number of enhancements to its documentation, systems, resourcing and training relevant to compliance with its SMR obligations, as referred to in paragraph 110 below;

(c) in accordance with CBA's Program and its supporting documents, processes, systems and controls (as amended from time to time):

(i) during the period from 1 January 2012 to 31 December 2017, CBA actioned approximately 234,000 alerts and filed over 44,000 SMRs;

(ii) CBA filed at least 259 SMRs in relation to the 127 customers the subject of the SMR and customer due diligence contraventions and at least 264 SMRs in relation to the 130 customers the subject of the Proceedings;

(d) during the period in question CBA provided intelligence direct to law enforcement and provided assistance in relation to police investigations, including in respect of a number of the customers the subject of the contraventions;

(e) the contraventions based on the "3 month policy" occurred in the circumstances described at paragraph 55(a) above and in a number of instances an SMR providing this information was subsequently filed; and

(f) the contraventions based on a misapprehension about the proper treatment of law enforcement information arose in the period between March 2015 and June 2017 and occurred in the circumstances described at paragraphs 55(b) and 55(c) above. In each case, CBA provided information or documents to some law enforcement units. In the contraventions relating to suspicions of false identity, CBA filed SMRs in respect of related concerns about transactional activity although failed also to note the false identity concerns.

CBA also acted on the information from law enforcement to prevent further transaction on these accounts.

84 Since these contraventions were identified, CBA has undertaken a range of further enhancements in respect of its SMR processes, systems and controls, as set out in paragraph 121 below and following.

**Customer Due Diligence**

85 CBA's admitted contraventions in respect of failures to undertake appropriate due diligence on particular customers (either for a certain period of time or, in some instances, at all) date from 15 December 2011 (at which point the maximum penalty was $11 million for each contravention) to 1 February 2018 (at which point the maximum penalty was $21 million for each contravention). The majority of CBA's admitted contraventions fall between August 2015 and June 2017, during which period the maximum penalty was $18 million for each contravention.

86 None of the contraventions was the result of a deliberate intention to breach the AML/CTF legislation.

87 The contraventions were serious because:

(a) CBA took insufficient risk-based steps to monitor these customers or undertake appropriate ECDD (as applicable) in spite of warning signs indicating high ML/TF risk. These warning signs included advice from law enforcement of accounts being investigated in connection with money laundering syndicates; CBA's own transaction monitoring alerts and SMRs; and detailed analysis from its own intelligence team. The systemic issues compounded the failure to assess the ML/TF risk of IDMs and the failure to align risk-based systems and controls with these risks.

(b) In some instances, no transaction monitoring alerts were raised for suspicious activity and, when alerts were raised, they were not reviewed in a timely manner having regard to ML/TF risk. In some instances, alerts were not reviewed for months after they were raised. In some instances, alerts were reviewed without regard to intelligence, both internal and external received from law enforcement.

(c) For some customers, CBA was slow to decide whether or not to continue doing business with such individuals. Rather, once suspected money laundering or structuring had been identified on these accounts, CBA sometimes looked no further than whether or not to submit an SMR without taking appropriate enhanced due diligence measures. This facilitated further money laundering.

(d) Where decisions were ultimately made to close accounts, the customers were given 30 days' notice. In 20 cases, money laundering continued during this notice period, without enhanced monitoring in place to ensure that it was detected and addressed promptly.

(e) CBA failed to put a timely stop on 1 account in respect of which it had formed suspicions of terrorism financing, during which time the customer attempted further transactions.

(f) The failure to properly monitor customers meant that emerging ML/TF risks were not adequately identified for the purposes of the ongoing identification, mitigation and management of the risks posed by the IDM channel, as required by the AML/CTF Program and s 82.

(g) The failure to properly monitor some of these customers meant that some matters that should have been flagged and reported as suspicious under s 41 were not identified.

(h) CBA's failure to sufficiently monitor or undertake appropriate ECDD in respect of the 80 customers (as applicable), for the purposes of s 36 facilitated money laundering by drug importation and distribution syndicates in the several millions of dollars.

88 The contraventions came about in circumstances where:

(a) at all material times:

(i) CBA's Program was in place, which included a system for complying with CBA's customer due diligence obligations (including through the Transaction Monitoring Program, OCDD Program and ECDD Program as well as a range of supporting Group Standards, Standard Operating Procedures, User Guides and Reference Guides), as referred to in paragraphs 18 to 20 above.

(ii) CBA applied the OCDD Program (including the Transaction Monitoring Program and ECDD Program) to its customers, including the customers the subject of the customer due diligence contraventions. This is a substantial enterprise. At present, CBA has approximately 16.6 million customers and processes over 16 million transactions per day.

(iii) CBA undertook customer due diligence and monitoring through its AML Operations team, including through its Transaction Monitoring and Customer Risk teams, as referred to in paragraph 21 above. Similar to the Transaction Monitoring team, the Customer Risk

team was overseen by the Managers in that team and the Executive Manager, AML/CTF Operations, Group Operations – Financial Crime and was co-located with the Transaction Monitoring team at the central operations centre.

(iv) The Transaction Monitoring and Customer Risk teams received both formal and informal training and education, including:

A. compulsory training in respect of the AML/CTF Act and Rules, CBA's reporting and customer monitoring obligations, typologies and offence types, use of Pegasus and other tools available to the teams for the purpose of transactional and customer analysis (such as CommSee, World Check) and ad hoc additional areas of focus;

B. regular internal team meetings to share information and discuss issues identified during transactional or customer reviews or alerts, feedback and quality assurance and AUSTRAC typologies as and when released;

C. email directives to communicate specific guidance to the teams in respect of, for example, instructions, feedback from outcomes of quality assurance and implementation of updates or changes to revised policies and procedures; and

D. ongoing feedback and coaching to provide assurance training and feedback following quality assurance reviews and general capability uplift.

(b) over the contravention period, and particularly from December 2015 onwards, CBA made a number of enhancements to its documentation, systems, resourcing and training relevant to customer due diligence, as referred to in paragraphs 121 to 124 below; and

(c) in accordance with CBA's Program and its supporting documents, processes, systems and controls, in the period from 1 January 2012 to 31 December 2017, the Transaction Monitoring team reviewed approximately 234,000 alerts and filed over 44,000 SMRs and between 1 July 2012 and 31 December 2017 it exited more than 4,800 customers. Among these, the Transaction Monitoring team reviewed alerts and filed SMRs in respect of the customers the subject of these Proceedings as follows:

| | **Customers** | **Alerts (automated and manual)** | **SMRs filed*** |
|---|---|---|---|
| **Syndicate 1** | 30 | 190 | 71 |
| **Syndicate 2** | 12 | 53 | 17 |
| **Syndicate 3** | 1 | 20 | 4 |
| **Syndicate 4** | 11 | 35 | 16 |
| **Cuckoo Smurfing Syndicate** | 18 | 33 | 26 |
| **Strike Force B** | 52 | 146 | 116 |
| **Remaining customers** (referred to in the Amended Statement of Claim as Persons 56, 75 and 136-139) | 6 | 25 | 14 |
| **TOTAL** | **130** | **502** | **264** |

*Note that some of these SMRs covered multiple customers or issues.

89 Since these contraventions were identified, CBA has undertaken a range of further enhancements in respect of its customer due diligence documentation, processes, systems and controls including as detailed in paragraph 110 below.

**E.2 Loss or damage suffered**

90 During the relevant period, CBA operated a high volume business, including operating for significant periods of time without having conducted risk assessments or implementing sufficient appropriate risk-based controls on its IDM channel. During this period, some of the customers the subject of the SMR and customer due diligence contraventions have been prosecuted and convicted of unlawful activity.

91 CBA failed to report millions of dollars of suspected money laundering activity through the timely provision of SMRs. During the period for which CBA admits that its monitoring and ECDD was deficient, several million dollars' worth of further unlawful activity was not detected. AUSTRAC suspects that there was significant further undetected money laundering through CBA accounts that ought to have been detected and reported.

92 The money laundered through the CBA accounts included the proceeds of drug and firearms importation and distribution syndicates – predominantly involving

methamphetamine. Criminal syndicates rely upon money laundering syndicates to import and distribute their drugs.

93 The late TTRs and the failures to report SMRs, on time or at all, have deprived AUSTRAC and law enforcement of intelligence to which they are entitled involving movements of several million dollars in cash. AUSTRAC and law enforcement were denied timely intelligence on about $625 million in threshold transactions and on several million dollars in suspicious activity.

**E.3 Prior contraventions**

94 CBA has not previously been found to have engaged in any contravention of the AML/CTF Act.

**E.4 CBA's size and financial position**

95 Details of CBA's size and financial position are set out in Section B.2 above.

96 CBA is a very well-resourced and sophisticated ASX 100 company which consistently earns profit in the billions, for example earning a $9.9 billion profit after tax in the last financial year.

**E.5 Board and senior management involvement**

97 CBA acknowledges that the AML/CTF Rules require ongoing oversight of Part A of CBA's Program by the Board and senior management.

98 During the contravention period:

(a) the Board received reports from senior management in relation to AML/CTF compliance, which contained input from personnel with direct responsibility for and oversight of the AML/CTF function; and

(b) CBA's senior management received reports in relation to AML/CTF compliance from personnel engaged in direct responsibility and oversight of the AML/CTF function and oversaw a range of measures directed to enhancing its AML/CTF function, including measures described further in Section E.7 below.

99 CBA now acknowledges that it did not take all necessary steps to appropriately identify, mitigate and manage the ML/TF risks of IDMs.

100 CBA acknowledges that there were deficiencies in oversight, accountabilities and resources in respect of its AML/CTF compliance and risk management functions.

101 In recognition of the importance of compliance with CBA's AML/CTF obligations and the collective responsibility of the Board and senior management, CBA reduced the director fees for non-executive directors by 20% in the 2018 financial year and

reduced to zero the Short Term Variable Remuneration outcomes for the CEO and group executives for the financial year ended 30 June 2017.

**E.6 Cooperation with AUSTRAC and contrition**

102 At all times, CBA has invested in building a productive, cooperative and transparent relationship with AUSTRAC. For example:

(a) throughout the relevant period, CBA and AUSTRAC representatives have met regularly for CBA to provide status updates on CBA's AML/CTF compliance and for AUSTRAC to provide feedback;

(b) throughout the relevant period, there have been numerous other instances of collaboration and information sharing between CBA and AUSTRAC, ranging from informal updates through to a visit from the AUSTRAC CFO to the AML Operations team centre and meetings between the AUSTRAC CEO and the CBA Board;

(c) following the identification of the TTR issue described at Section C.2 above, CBA responded swiftly to identify the root causes and scope a remediation program and communicate this to AUSTRAC, and thereafter CBA engaged with AUSTRAC promptly and cooperatively in respect of its further enquiries;

(d) CBA was a founding member, and is a Board member, of the Fintel Alliance, which is a private-public partnership led by AUSTRAC and designed to help the private sector more easily identify and report suspicious transactions and help law enforcement to arrest and prosecute criminals quickly. CBA has been recognised by AUSTRAC for its support and assistance to the Fintel Alliance; and

(e) in early 2017, one of CBA's senior financial crime personnel attended, at AUSTRAC's invitation:

(i) the Financial Action Task Force's Joint Experts Meeting in Moscow in 24-27 April 2017 regarding the promotion of effective implementation of legal and regulatory measures for combating money laundering, terrorism financing and other related threats to the integrity of the international financial system; and

(ii) a meeting with an overseas AML/CTF expert to discuss a study being conducted in relation to the "Typologies of the Financing of Proliferation" funded by the US State Department.

103 Since the commencement of these Proceedings:

(a) CBA has continued to work cooperatively with AUSTRAC on matters relating to AUSTRAC's ongoing supervisory role and in the conduct of the Proceedings; and

(b) CBA entered all of the admissions in Section D above at the earliest available opportunity.

104 Further, CBA:

(a) agrees that money laundering and terrorism financing undermine the integrity of the Australian financial system and impact the Australian community's safety and wellbeing;

(b) acknowledges that, as a bank, CBA plays a key role in combatting money laundering and terrorism financing;

(c) accepts its accountability for the admitted contraventions;

(d) expresses its deep regret for those contraventions;

(e) acknowledges the significant impact that deficiencies in its systems and processes can have on efforts to combat money laundering and terrorism financing;

(f) accepts that it needs to be ever vigilant in this area; and

(g) emphasises its commitment to working with AUSTRAC and law enforcement agencies to fight money laundering and counter terrorism financing.

## E.7 Corrective Measures and enhancements

### Outline of activities directed to AML/CTF enhancements

105 CBA has advised AUSTRAC that it has undertaken the following activities.

106 Since 2010, CBA has invested more than $400 million on AML/CTF compliance, including expenditure on upgrading and enhancing its AML/CTF technology, updating its process documentation, investing in further resourcing and strengthening training of its personnel.

107 Reflecting its scale, size of customer base and spread of geographic operations, the systems and controls to support CBA's AML/CTF compliance are of such a scale and complexity that effecting changes, upgrades and enhancements is necessarily time consuming and work must be undertaken carefully having regard to achieving the optimal outcome and the possibility of unintended consequences.

108 In around 2014, CBA commenced a significant and complex technology project to upgrade the hardware and software of the FCP with a view to substantially expanding the capability of the FCP including for CBA's Transaction Monitoring Program. Given

its scale and complexity, the design and implementation activities associated with the project occurred over a number of years. Work commenced on the upgrade in late 2016, and it has been substantially complete since January 2018 at a total cost of more than $36 million.

109 In around 2015, CBA also undertook a significant project of work to prepare CBA's systems and controls to accommodate upcoming AML/CTF regulatory change, including investment in training and compliance monitoring.

110 From mid-2015 onwards, CBA made a number of enhancements to its AML Operations team and associated documentation, systems, processes and controls related to its SMR and customer due diligence obligations. These are addressed in paragraphs 121 to 124 below. In or around mid-2015, CBA took additional steps to strengthen its AML/CTF function including by hiring experienced new staff into senior policy, advisory and assurance positions.

111 In April 2016, CBA moved to consolidate financial crime personnel into a Line 1 'Financial Crime (Anti-Money Laundering, Counter Terrorism Finance, Anti-Bribery & Corruption and Sanctions) Centre of Excellence' model (**Financial Crime Centre of Excellence**), with the intention of improving the organisational design of CBA's AML/CTF function so as to better facilitate end-to-end oversight of AML/CTF compliance. The Financial Crime Centre of Excellence became part of Group Security.

112 Following the establishment of the Financial Crime Centre of Excellence, CBA's Group Standards relating to AML/CTF issues were updated and enhanced in 2016 as part of an upgrade project by personnel responsible for AML/CTF policy matters. As part of this, CBA reviewed its risk assessment processes and created a risk assessment tool, as described in paragraph 64(d) above.

113 Since the Proceedings commenced, CBA has advised AUSTRAC that it has continued to implement AML/CTF enhancements.

114 The enhancements that have been made to CBA's AML/CTF processes, systems and controls include:

(a) undertaking further adjustments to the structure of its AML/CTF function by strengthening reporting lines and appointing additional senior personnel into AML/CTF roles, including an experienced Executive General Manager of Financial Crimes Compliance on 5 March 2018;

(b) significantly expanding the Financial Crimes Compliance team (including the AML Operations team);

(c) adjusting reporting lines and improving the quality of AML/CTF information being circulated (including to Board and senior management) in order to enhance governance and reporting processes;

(d) introducing further automated transaction monitoring rules and enhancing its governance processes for considering and implementing further rules; and

(e) undertaking a large-scale assessment and refresh of its financial crime training program with a focus on building financial crime capability across CBA. This includes tailored programs for specific business units and teams within CBA where those personnel have responsibility for certain transaction monitoring activities or suspicious matter reporting, engage with customers, or are in senior positions.

115 CBA has also made a number of enhancements specific to the areas of contravention as described below.

**Risk Assessments**

116 In addition to the enhancements referred to in paragraph 64 above, CBA has introduced a number of enhancements specifically to further identify, mitigate and manage its ML/TF risk in respect of IDMs as follows:

(a) CBA undertook a further ML/TF risk assessment specific to IDMs, which was approved on 23 October 2017. In that risk assessment, CBA assessed the IDMs to have a high inherent ML/TF risk and recorded its intention to introduce daily limits on IDM cash deposits.

(b) On 21 November 2017, CBA implemented a daily limit of $20,000 to holders of CBA branded cards connected with a personal account when depositing cash through IDMs;

(c) CBA refreshed its ML/TF risk assessment specific to IDMs in March 2018. CBA decided to impose a $10,000 account based daily limit on cash deposits through IDMs to CBA personal and business accounts, subject to accounts of certain business customers and institutional banking customers having a higher limit;

(d) On 12 April 2018, CBA implemented a daily limit of $10,000 to CBA personal and business accounts. This control operates at an *account based* (rather than card based) level, and prevents a CBA account from receiving a cash deposit of more than $10,000 per day through an IDM. These account based daily limits apply to all CBA customers who have personal or business accounts, with some exceptions for business accounts. Those exceptions relate to business accounts for certain Business & Private Banking and Institutional Banking & Markets customers, where the relevant business account holders have been assessed as having a business need to deposit larger volume cash takings at IDMs (for example, retail businesses whose employees may need to deposit cash takings outside of branch hours and

where it would present a safety risk for the business, or its employees, to keep hold of cash);

(e) CBA communicated with the Branch network to inform Branch staff of the implementation of daily limits in IDMs and reminded Branch staff to be alert for typologies of behaviours they should report as STRs, including cash structuring;

(f) CBA developed and implemented additional transaction monitoring rules relating specifically to IDMs; and

(g) CBA implemented additional systems and controls, for example the introduction of a system for the manual monitoring of cash deposits through IDMs.

117 CBA has also made further enhancements to its systems, processes and controls, for example, the following additional measures have been implemented:

(a) The Retail Banking Services (**RBS**) team has responsibility for IDMs and has introduced a dedicated RBS Financial Crime team for managing and overseeing financial crime matters that arise in connection with the designated services offered by that Business Unit including ML/TF risk assessments. This team reports to the General Manager for RBS Controls & Customer Outcomes; and

(b) RBS has also introduced an RBS Financial Crime Governance Forum which meets monthly to consider issues relating to financial crime. The RBS Financial Crime Governance Forum receives regular reporting, including in respect of both operational updates (such as transaction monitoring alert volumes, SMR volumes and other relevant data) and enhancements to RBS systems and controls. The RBS Financial Crime Governance Forum will also now receive ML/TF risk assessments for noting when a new RBS product is being launched or where substantial changes are being proposed in respect of an existing RBS product.

**Threshold Transaction Reporting to AUSTRAC**

118 Following its disclosure of the late TTR issue to AUSTRAC in September 2015, CBA also undertook an internal review for the purpose of identifying the cause of the issue. In doing so, CBA identified the systems relevant to the TTR process and established an engagement model between RBS and Enterprise Services (the team within CBA responsible for the systems used by the TTR process) to share information relating to potential changes to systems that might impact TTR processes.

119 Since that time, CBA has made further enhancements to its TTR processes, systems and controls. For example:

(a) in September 2017, CBA introduced a manual exception reporting process to identify all threshold transactions undertaken at an IDM and match them to corresponding TTRs. This process is designed to enable CBA to identify and rectify any issues with TTR reporting promptly should they occur, by reconciling transactions recorded in its systems with TTRs which are automatically prepared and identifying any discrepancies that may arise. RBS provides weekly reporting in respect of this exceptions process and any discrepancies that arise are addressed with a view to ensuring that any required TTRs are prepared and given to AUSTRAC within the statutory time frame;

(b) in October 2017, CBA introduced an assurance process in respect of the manual exception reporting process as a means to ensure the exceptions process was sufficient and robust;

(c) since in or about February 2018, CBA monitors the monthly volume of TTRs, which monitoring demonstrates that since August 2017, CBA has submitted between 60,000 and 80,000 TTRs to AUSTRAC per month; and

(d) CBA has determined clear accountabilities for the timely and accurate submission of TTRs to AUSTRAC.

**Transaction Monitoring Program**

120 CBA has implemented substantial enhancements to the processes, systems and controls supporting its Transaction Monitoring Program, including as set out below:

(a) CBA now conducts weekly monitoring of data in the FCP to detect any instances where the 'account type description' field (which is required for automated transaction monitoring to operate as intended) is not populated;

(b) as discussed at paragraph 108 above, CBA has undertaken a significant project to upgrade the FCP, enabling CBA to enhance its capacity to undertake automated transaction monitoring of its customers; and

(c) CBA has strengthened its accountability and governance in respect of the FCP.

**Suspicious matter reporting to AUSTRAC and customer due diligence**

121 From around mid-2015 onwards, CBA has undertaken a range of enhancements to the structure, resourcing and capabilities of its AML Operations team. For example:

(a) in around March 2016, responsibility for AML and Sanctions operations was divided in two, with each having its own dedicated Executive Manager;

(b) CBA has significantly expanded the size of its AML Operations team. The AML Operations team was expanded in late 2015. The team has since

expanded further. The Transaction Monitoring team currently has the equivalent of 78 full time Analysts and 18 full time Senior Analysts as well as 4 newly created subject matter expert positions to further strengthen the capability of the team. The Customer Risk team currently has the equivalent of 47 full time Analysts and 12 full time Senior Analysts as well as 2 newly created subject matter expert positions to further strengthen the capability of the team.

(c) in addition to the training and oversight referred to at paragraph 87(a)(iv) above, enhancements were introduced within both the Transaction Monitoring team and Customer Risk team from the second half of 2015, including:

(i) comprehensive compulsory training and ongoing quality assurance processes for new starters;

(ii) daily team meetings to cover operational and performance matters and to share information and observations, including common trends, assurance issues and best practice; and

(iii) regular specific role-based training of the Transaction Monitoring team and Customer Risk team directed at capability uplift, feedback and improving quality, including the introduction of intensive "spotlight sessions" provided on a monthly basis to the Transaction Monitoring team focussing on key areas following outcomes of quality assurance.

122 CBA has also enhanced its processes for ensuring that frontline staff and personnel in other parts of the business identify and pass on relevant information to the AML Operations team in a timely manner, for consideration as part of its SMR and customer due diligence responsibilities. For example:

(a) in late 2017, CBA introduced a simplified and updated eForm for staff to complete when they identified unusual activity for drawing to the attention of the AML Operations team (known as the 'STR eForm'); and

(b) from around February 2017, CBA introduced progressive enhancements to its processes for ensuring that relevant information from law enforcement was provided to the AML Operations team in a consistent and timely manner, including through the introduction of dedicated resources to assist the Compliance Services team to lodge STRs where necessary. There are presently dedicated personnel for ensuring that relevant law enforcement communications received by the Compliance Services team are identified and that appropriate STRs are completed.

123 In addition to the enhancements described above, CBA has made a number of enhancements specifically directed to compliance with its SMR obligations, including to address matters directly relevant to the SMR contraventions. For example:

(a) in December 2016, CBA updated its Group Standard in respect of SMR obligations, now known as the "Transaction Monitoring and AUSTRAC Suspicious Matter Reports Group Standard". That Group Standard provided further detail and guidance as to CBA's approach to meeting its SMR obligations, including by setting out:

(i) the prioritisation of review of alerts by Transaction Monitoring team analysts;

(ii) the necessary information required to be included in an SMR;

(iii) reporting of transactions and patterns of behaviour suggestive of structuring;

(iv) further examples and indicators of circumstances which may give rise to a reporting obligation.

It also emphasised the need to submit an SMR "in each and every instance an SMR obligation arises";

(b) CBA has provided clear directives to its Transaction Monitoring team in that the approach described at paragraph 55(a) above is no longer to be used. It has also used the daily team meetings referred to in paragraph 121(c)(ii) above to emphasise the need for <u>all</u> suspicions to be fully and accurately reported; and

(c) CBA has also provided further guidance to its Transaction Monitoring team in respect of incorporating relevant information from law enforcement communications into SMRs.

124 Further, CBA has made a number of additional enhancements specifically directed to compliance with its customer due diligence obligations, including to address matters directly relevant to the customer due diligence contraventions. For example:

(a) CBA has substantially reduced the target time frames in which the Transaction Monitoring and Customer Risk teams are expected to (and do) review Automated TM Alerts, Manual Alerts and HRC alerts (as applicable). CBA understands its target time frames for reviewing transaction monitoring alerts, as at 1 December 2017, to be significantly shorter than industry standard.

(b) CBA has introduced more regular, formal monitoring of its performance for reviewing alerts against its targets. From September 2017, information

tracking review times against targets has been prepared on a daily basis in a report known the Financial Crime Operations (**FCO**) Daily SLA report (**FCO Daily Report**). The FCO Daily Report is provided to various personnel in senior management.

(c) CBA has introduced a range of enhancements to its ECDD documentation, processes, systems and controls. For example:

(i) In late 2015, CBA prepared a stand-alone ECDD Group Standard which was formally approved in January 2016. This Group Standard specified the minimum ECDD measures to be taken in relation to every customer in respect of which an ECDD trigger had arisen, and required consideration of whether an SMR needed to be submitted to AUSTRAC at the completion of the ECDD process.

(ii) In December 2015, shortly prior to the ECDD Group Standard being approved, CBA introduced an ECDD Reference Guide to provide guidance on each of the ECDD measures required by the ECDD Group Standard.

(iii) In and from December 2015, CBA introduced a stand-alone ECDD standard operating procedure (**ECDD SOP**) detailing the necessary steps required to be followed when completing ECDD to ensure that alerts are actioned correctly and consistently. This SOP included a template document "ECDD Customer Case Summary" that was required to be completed by Analysts in the AML Operations Team to record ECDD steps undertaken in respect of a customer and the results of those steps. The ECDD SOP was subsequently reviewed and refined in May 2016 and March 2017.

(iv) From December 2015, CBA refined its ECDD process such that each time an SMR was submitted for a customer, an HRC alert was sent to the Customer Risk team for further analysis.

(v) From around the same time, CBA undertook a series of progressive refinements to its customer termination processes, including the introduction of the Customer Risk Termination SOP which sets out the circumstances in which a customer relationship should be terminated, how approval to terminate is sought and the time frame for the business unit to provide approval to terminate.

(vi) Since the commencement of these Proceedings, CBA has undertaken further work to strengthen its termination processes and controls for RBS customers, including:

A. expediting customer account closures based on ML/TF concerns, through the introduction of significantly reduced notice periods;

B. implementing controls to mitigate and manage the risk of further suspicious or unusual transactional activity occurring during the reduced termination notice periods; and

C. establishing a Customer Exit Committee to be responsible for dealing with complex customer exit decisions (for example, where a customer has a business relationship with multiple business units).