

NOTICE OF FILING

Details of Filing

Document Lodged:	Statement of Agreed Facts
Court of Filing	FEDERAL COURT OF AUSTRALIA (FCA)
Date of Lodgment:	30/05/2023 11:21:36 AM AEST
Date Accepted for Filing:	30/05/2023 11:21:46 AM AEST
File Number:	NSD134/2022
File Title:	CHIEF EXECUTIVE OFFICER OF THE AUSTRALIAN TRANSACTION REPORTS AND ANALYSIS CENTRE v CROWN MELBOURNE LIMITED ACN 006 973 262 & ANOR
Registry:	NEW SOUTH WALES REGISTRY - FEDERAL COURT OF AUSTRALIA



Sia Lagos

Registrar

Important Information

This Notice has been inserted as the first page of the document which has been accepted for electronic filing. It is now taken to be part of that document for the purposes of the proceeding in the Court and contains important information for all parties to that proceeding. It must be included in the document served on each of those parties.

The date of the filing of the document is determined pursuant to the Court's Rules.



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

No. NSD 134 of 2022

Chief Executive Officer of the Australian Transaction Reports and Analysis Centre
Applicant

Crown Melbourne Limited
ACN 006 973 262
First Respondent

Burswood Nominees Ltd as trustee for The Burswood Property Trust trading as Crown Perth
ACN 078 250 307
Second Respondent

STATEMENT OF AGREED FACTS AND ADMISSIONS

Table of contents

A.	INTRODUCTION	3
B.	PARTIES AND BACKGROUND	3
	B.1 AUSTRAC	3
	B.2 Crown Melbourne and Crown Perth	3
	B.3 Designated services	4
	B.4 Overview of the key concepts underlying the AML/CTF Act	5
C.	GAMING SERVICES AND FINANCIAL SERVICES	7
	C.1 Membership	7
	C.2 Gaming locations	7
	C.3 Gaming types	8
	C.4 Financial services and the funding of gaming activities	8
	C.5 Turnover, revenue and profit	13
	C.6 Junkets	13
D.	RELEVANT OBLIGATIONS UNDER THE AML/CTF ACT	15
E.	CROWN MELBOURNE'S AND CROWN PERTH'S AML/CTF PROGRAMS	20
	E.1 Crown Melbourne Standard Program	20
	E.2 Crown Perth Standard Program	21
	E.3 Crown Joint AML/CTF Program	22
F.	CROWN'S CONTRAVENTIONS OF SECTION 81 OF THE AML/CTF ACT – STANDARD AND JOINT PROGRAMS	23
	F.1 Risk assessments	23

F.2	Board and senior management oversight	30
F.3	Remittance services, Credit Facilities and CCFs	32
F.4	Risk-based systems and controls	39
F.5	Junkets	48
F.6	Transaction monitoring programs	59
F.7	Enhanced Customer Due Diligence Programs	64
F.8	Reporting obligations	70
F.9	Applicable Customer Identification Procedures (ACIPs)	74
F.10	Joint AML/CTF Program	78
F.11	Conclusion	82
G.	CROWN'S CONTRAVENTIONS OF SECTION 36 OF THE AML/CTF ACT	82
G.1	High risk customers	83
G.2	Typology customers	91
G.3	Contraventions	93
H.	FACTS RELEVANT TO RELIEF	93
H.1	Nature and extent of the contraventions	93
H.2	Loss or damage suffered	99
H.3	Prior contraventions	101
H.4	Crown's size and financial position	101
H.5	Board and senior management involvement	105
H.6	Cooperation with AUSTRAC and contrition	105
H.7	Remediation, corrective measures and enhancements	106
H.8	Other facts relevant to deterrence	111

Chief Executive Officer of the Australian Transaction Reports and Analysis Centre
Applicant

Crown Melbourne Limited
ACN 006 973 262
First Respondent

Burswood Nominees Ltd as trustee for The Burswood Property Trust trading as Crown Perth
ACN 078 250 307
Second Respondent

A. INTRODUCTION

- 1 This Statement of Agreed Facts and Admissions (**SAFA**) is made for the purposes of section 191 of the *Evidence Act 1995* (Cth), jointly by the Applicant (the Chief Executive Officer (**CEO**) of the Australian Transaction Reports and Analysis Centre (**AUSTRAC**)), and the Respondents, Crown Melbourne Limited (**Crown Melbourne**) and Burswood Nominees Ltd as trustee for the Burswood Property Trust trading as Crown Perth (**Crown Perth**, and, together with Crown Melbourne, **Crown**).
- 2 The AUSTRAC CEO has sought declarations that Crown contravened particular provisions of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (**AML/CTF Act**) and an order that it pay a pecuniary penalty to the Commonwealth.
- 3 Crown Melbourne and Crown Perth each admit that they contravened sections 36(1) and 81(1) of the AML/CTF Act in the particular respects as set out in this SAFA. This SAFA identifies the facts relevant to the contraventions admitted by Crown. The facts agreed to, and the admissions made, are agreed to and made solely for the purpose of the proceeding and do not constitute an admission outside of the proceeding.

B. PARTIES AND BACKGROUND

B.1 AUSTRAC

- 4 The AUSTRAC CEO is appointed pursuant to section 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 proceeding in that capacity.

B.2 Crown Melbourne and Crown Perth

- 5 Crown is a provider of gambling and financial services within the meaning of the AML/CTF Act (see below).
- 6 Throughout the period 1 March 2016 to 1 March 2022 (the **Relevant Period**), Crown Resorts Limited (**Crown Resorts**) was the ultimate holding company of Crown Melbourne and

Burswood Limited (**Burswood Ltd**). Burswood Ltd is, and was during the Relevant Period, the holding company of Crown Perth. Since June 2022, the ultimate Australian holding company of Crown Melbourne and Burswood Ltd has been SS Silver Pty Ltd.

- 7 Crown Melbourne and Crown Perth are, and at all material times were:
- (a) incorporated in Australia;
 - (b) persons within the meaning of section 5 of the AML/CTF Act;
 - (c) reporting entities within the meaning of section 5 of the AML/CTF Act;
 - (d) providers of designated services to customers within the meaning of section 6 of the AML/CTF Act; and
 - (e) carrying on activities or business through a permanent establishment in Australia for the purposes of the AML/CTF Act.
- 8 At all material times, Crown Melbourne held a casino licence under Part 2 of the *Casino Control Act 1991* (Vic), and operated under the Casino Agreement between the Victorian Casino Control Authority and Crown Casino Limited dated 21 September 1993 (as amended).
- 9 At all material times, Crown Perth has held a casino licence under Part IV of the *Casino Control Act 1984* (WA), and has operated under the *Casino (Burswood Island) Agreement Act 1985* (WA) and the Casino (Burswood Island) Agreement between the State of Western Australia, West Australian Trustees Limited and Burswood Management Limited dated 20 February 1985 (as amended).

B.3 Designated services

- 10 The AML/CTF Act applies with respect to designated services. A person who provides a designated service is a reporting entity. Throughout the Relevant Period, Crown provided the following designated services pursuant to section 6 of the AML/CTF Act.

Financial services, table 1

- (a) Item 6, table 1 – making a loan as defined under section 5 of the AML/CTF Act, where the loan is made in the course of carrying on a loans business;
- (b) Item 7, table 1 – in the capacity of the lender for a loan, allowing the borrower to conduct a transaction in relation to the loan, where the loan was made in the course of carrying on a loans business;
- (c) Item 31, table 1 – in the capacity of a non-financier carrying on a business of giving effect to remittance arrangements, accepting an instruction from a transferor entity for the transfer of money or property under a designated remittance arrangement; and
- (d) Item 32, table 1 – in the capacity of a non-financier carrying on a business of giving effect to remittance arrangements, making money or property available, or arranging for it to be made available, to an ultimate transferee entity as a result of a transfer under a designated remittance arrangement;

Gaming services, table 3

- (e) Item 1, table 3 – receiving or accepting a bet placed or made by a person, where the service is provided in the course of carrying on a gambling business;

- (f) Item 4, table 3 – paying out winnings in respect of a bet, where the service is provided in the course of carrying on a gambling business;
- (g) Item 6, table 3 – accepting the entry of a person into a game where:
 - (i) that game is played for money or anything else of value;
 - (ii) the game is a game of chance or of mixed chance and skill;
 - (iii) the service is provided in the course of carrying on a gambling business; and
 - (iv) the game is not played on a gaming machine located at an eligible gaming machine venue;
- (h) Item 7, table 3 – exchanging money or digital currency for gaming chips / tokens / betting instruments, where the service is provided in the course of carrying on a business;
- (i) Item 8, table 3 – exchanging gaming chips / tokens / betting instruments for money or digital currency, where the service is provided in the course of carrying on a business;
- (j) Item 9, table 3 – paying out winnings, or awarding a prize, in respect of a game where:
 - (i) that game is played for money or anything else of value;
 - (ii) the game is a game of chance or of mixed chance and skill;
 - (iii) the service is provided in the course of carrying on a gambling business; and
 - (iv) the game is not played on a gaming machine located at an eligible gaming machine venue;
- (k) Items 11 to 13, table 3 – in the capacity of account provider:
 - (i) opening an account; or
 - (ii) allowing a person to be a signatory on an account; or
 - (iii) allowing a transaction to be conducted in relation to an account,

where the account provider is a person who provides a service covered by items 1, 2, 3, 4, 6, 7, 8 or 9 in table 3 of section 6 of the AML/CTF Act, and the purpose, or one of the purposes, of the account is to facilitate the provision of a service covered by items 1, 2, 3, 4, 6, 7, 8 or 9 in table 3 of section 6 of the AML/CTF Act, and the service is provided in the course of carrying on a business; and
- (l) Item 14, table 3 – exchanging one currency (whether Australian or not) for another (whether Australian or not), where the exchange is provided by a person who provides a service covered by items 1, 2, 3, 4, 6, 7, 8 or 9 in table 3 of section 6 of the AML/CTF Act, and the service is provided in the course of carrying on a business.

- 11 Section C from paragraphs 21 to 60 and 66 to 71 details the designated services provided by Crown during the Relevant Period.

B.4 Overview of the key concepts underlying the AML/CTF Act

- 12 An object of the AML/CTF Act is to provide for measures to detect, deter and disrupt money laundering, the financing of terrorism, and other serious financial crimes (section 3(1)(aa) of the AML/CTF Act).
- 13 The designated services provided by Crown involve money laundering and terrorism financing risks (**ML/TF risks**):

- (a) In addition to gaming services (table 3, section 6 of the AML/CTF Act), casinos provide financial services (table 1, section 6 of the AML/CTF Act), enabling customers to move money into and out of the casino environment (including domestically and internationally). This involves high ML/TF risks.
 - (b) Casinos are particularly vulnerable to money laundering, including because the nature of their business involves a significant amount of cash. It is difficult to trace the source and ownership of cash, and the proceeds of crime are often in cash.
 - (c) Customers of a casino can move money through different designated services, including:
 - (i) transferring money through cash, casino value instruments (**CVIs**) (such as chips and tickets) and gaming accounts;
 - (ii) transferring money to or from their own gaming account; and
 - (iii) drawing on or redeeming credit provided by the casino.
 - (d) The movement of money through different designated services at a casino can make it difficult to understand the purpose of transactions, the beneficial owner of the funds or the ultimate beneficiary. The movement of money through a casino can involve:
 - (i) long and complex transaction chains (such as those identified at (c) above); and
 - (ii) multiple channels, including non-face-to-face channels.
 - (e) Casinos may also provide designated services to customers who involve higher ML/TF risks, including customers transacting through junkets or VIP Programs, customers from foreign jurisdictions, and potentially foreign politically exposed persons (**PEPs**).
 - (f) Money laundering and terrorism financing (**ML/TF**) typologies are the various methods that criminals use to conceal, launder or move illicit funds. Set out at **Schedule 2** below are money laundering vulnerabilities and ML/TF typologies that were relevant to casinos during the Relevant Period.
- 14 As set out in Section D, to manage these ML/TF risks, the AML/CTF Act requires reporting entities to:
- (a) identify and assess the ML/TF risks it reasonably faces: see paragraphs 76 and 77;
 - (b) adopt and maintain an anti-money laundering and counter-terrorism program within the meaning of section 83 of the AML/CTF Act: see paragraphs 76 to 80; and
 - (c) carry out ongoing due diligence on customers of designated services: see paragraphs 72 to 75 and 78(j) to (o).
- 15 The AML/CTF Act does not require ML/TF risks to be eliminated. Nor does the AML/CTF Act prescribe exactly how a reporting entity is to manage its ML/TF risks. The AML/CTF Act reposes trust in reporting entities to design and implement risk management procedures, systems and controls to detect and deter ML/TF that are appropriate for its business and that it will adopt and maintain through its AML/CTF program.
- 16 As further set out at paragraph 78(a) and (b), in determining what risk management procedures, systems and controls are appropriate for its AML/CTF program, the AML/CTF Act and Rules require reporting entities to take into account certain matters, including:
- (a) the nature, size and complexity of its business; and
 - (b) the ML/TF risks it reasonably faces, having regard to:

- (i) the type of designated services it provides;
 - (ii) the type of customers it provides designated services to;
 - (iii) the methods through which it delivers designated services (known as **channels**); and
 - (iv) the foreign jurisdictions with which they deal.
- 17 An AML/CTF program will not include **appropriate risk-based procedures, systems and controls** that meet the requirement of the AML/CTF Act and AML/CTF Rules if:
- (a) it has not taken the matters set out at paragraph 16 into account when designing and adopting the procedures, systems and controls; and
 - (b) the procedures, systems and controls are not aligned and proportionate to the ML/TF risks reasonably faced having regard to the matters set out at paragraph 16(b).
- 18 The AML/CTF Act and Rules require reporting entities to have regard to the matters set out at paragraph 16 when determining what ongoing customer due diligence (**OCDD**) is appropriate for its customers (see paragraph 78(j)).

B.5 Overview of Crown's contraventions of the AML/CTF Act

- 19 Crown admits that during the Relevant Period:
- (a) its AML/CTF programs did not meet the requirements of the AML/CTF Act and AML/CTF Rules (see Section F.11); and
 - (b) it did not carry out appropriate OCDD with respect to 505 customers, resulting in 546 contraventions of section 36(1) of the AML/CTF Act (see Section G.3).
- 20 Crown admits that the contraventions set out at paragraph 19 made Crown vulnerable to criminal exploitation and exposed the Australian community and financial systems to ML/TF risks (see section H.1 and H.2).

C. GAMING SERVICES AND FINANCIAL SERVICES

- 21 Crown offered, and continues to offer, a wide range of gaming services and a number of financial services to customers within the scope of tables 1 and 3, section 6 of the AML/CTF Act, either as members or non-members.

C.1 Membership

- 22 During the Relevant Period, customers wanting to become members had to complete an application process, which included the customers being identified. Members were able to access benefits, including applying for a Crown Rewards card, which allowed members to earn points from gaming and other expenditure. These points could be redeemed for gaming or rewards (for example, food and beverages). Depending on the level of gaming activity, members could attain different tiers of membership, which offered them access to increasing levels of rewards and certain Crown facilities.

C.2 Gaming locations

- 23 Crown primarily provided gaming services on the main gaming floors, which were accessible to all customers. In addition, both venues offered private or VIP areas to members based on their membership tier. A list of these areas is set out at **Schedule 1**.

C.3 Gaming types

- 24 Throughout the Relevant Period, Crown offered a wide range of games that involved the provision of designated services under table 3, section 6 of the AML/CTF Act, including:
- (a) Table Games – games offered at tables on the main gaming floor and in private rooms, including baccarat, roulette, blackjack, Sic Bo, poker and others;
 - (b) Electronic Table Games (**ETGs**) – semi and fully automated versions of traditional table games, where customers played at terminals; and
 - (c) Electronic Gaming Machines (**EGMs**) – themed games played on electronic machines.
- 25 Crown provided designated services under items 6 and 9, table 3, section 6 of the AML/CTF Act with respects to these games.

C.4 Financial services and the funding of gaming activities

- 26 Throughout the Relevant Period, Crown Melbourne and Crown Perth also provided financial services, within the meaning of table 1, section 6 of the AML/CTF Act, that facilitated the movement of money into and out of the casino environment, including across international borders. They also provided gaming accounts to customers, within the meaning of table 3, section 6 of the AML/CTF Act, to facilitate the funding of gaming activity (items 11 and 13, table 3, section 6 of the AML/CTF Act). Gaming activity could also be funded through chips, tokens or betting instruments, within the meaning of table 3, section 6 of the AML/CTF Act, also known as CVIs (items 7 and 8, table 3, section 6 of the AML/CTF Act).

The Cage

- 27 Depending on the game played, customers were able to fund their gaming activities in a variety of ways, including cash, cheque, telegraphic transfer, credit and cheque cashing facilities, chips and other CVIs (as outlined below). Central to the funding of gaming activity was the **Cage**, which operated as the 'bank' of the casino, and managed the monetary transactions between customers and the casino in relation to gaming. Crown had multiple cashier windows in various locations in the venues, at which customers could conduct transactions. The Cage also processed some monetary transactions that Crown customers could conduct non-face-to-face, as described in paragraph 37.

Crown Patron Accounts

- 28 Crown Melbourne and Crown Perth maintained bank accounts (**Crown Patron Accounts**) in AUD and foreign currencies to facilitate the transfer of funds into Crown to fund gaming activity by customers. Funds deposited into Crown Patron Accounts by or on behalf of customers were recorded on a ledger on SYCO¹ with reference to a customer's gaming account. These gaming accounts, as explained below, were known as deposit accounts (**DABs**) and safekeeping accounts (**SKAs**).
- 29 Crown Patron Accounts facilitated the movement of funds both domestically and internationally. Funds could be deposited into a Crown Patron Account by cash, cheque or telegraphic transfer, in Australian dollars or foreign currency. These deposits were credited to a customer's DAB or

¹ SYCO was the information management system jointly used by Crown Melbourne and Crown Perth to record gaming activity, buy-in and pay-out or cash-out transactional data, cashier activity, customer account transactions and credit control functions. It was also the system that interfaced with and captured data from other Crown systems, generated manual reports for transaction monitoring purposes and generate XML files for bulk uploads to AUSTRAC of reports required under Part 3 of the AML/CTF Act.

SKA and involved the provision of item 32, table 1, and item 13, table 3, section 6 designated services.

- 30 A customer of Crown Melbourne or Crown Perth could:
- (a) deposit funds personally into a Crown Patron Account;
 - (b) arrange for any third party to deposit funds into a Crown Patron Account, until November 2020, when policies to prohibit third party transactions (with limited exceptions) started to be introduced by Crown Melbourne and Crown Perth;
 - (c) instruct certain other casinos (Australian and foreign) to transfer a customer's funds from their non-Crown casino account into a Crown Patron Account until May 2021; and
 - (d) instruct another Crown entity to deposit funds into a Crown Patron Account on their behalf.
- 31 Crown Patron Accounts were used by some third party entities (such as junket tour operators, remittance service providers and overseas deposit services, as described further below) to make deposits on behalf of Crown Melbourne and Crown Perth customers.
- 32 Crown Patron Accounts also facilitated the payment of winnings to customers or the return of funds not used for gaming. These payments were facilitated by the transfer of customer funds from a DAB or SKA to a bank account nominated by the customer (which could be the customer's personal bank account; or until November 2020, a third-party bank account or a bank account of another casino). These transfers were debited from a customer's DAB or SKA and involved the provision of item 31, table 1, and item 13, table 3, section 6 designated services.
- 33 Crown Patron Accounts held in the name of Southbank Investments Pty Ltd (**Southbank**) (wholly owned and operated by Crown Melbourne) and Riverbank Investments Pty Ltd (**Riverbank**) (wholly owned by Burswood Ltd and operated by Crown Perth) were used to accept funds for or on behalf of Crown customers. These accounts were closed in December 2019.

DABs and SKAs

- 34 Customers were able to establish a DAB with Crown, which was a general ledger account in the name of a customer that was used for day-to-day casino transactions. Transactions on DABs and SKAs involved item 13, table 3, section 6 designated services.
- 35 Customers were able to credit their DAB by depositing monies in cash, cheque or by telegraphic transfer into Crown Patron Accounts (see paragraphs 28 to 33 above). Customers were also able to credit their DAB by making a deposit at the Cage in cash, chips, ticket-in and ticket-out tickets (**TITO**) and other CVIs. Prior to November 2020, funds could also be deposited into a customer's DAB by way of transfer from another DAB, held either by the customer or a third party. Transfers between customers' DABs also involved items 31 and 32, table 1, section 6 designated services.
- 36 Customers could withdraw money from a DAB in the form of cash, cheque, telegraphic transfer to a bank account, chips or other CVIs.
- 37 Generally, when a customer wanted to access funds from their DAB for gaming, they had to present themselves at a Cage cashier window, where their identity was verified by Cage staff,

and they were able to draw on funds credited to their DAB.² The withdrawal details were recorded in the DAB records in Crown's systems. In some circumstances, customers (or third parties) could also withdraw funds from DABs through non-face-to-face channels, without being present at the Cage (see paragraph 189).

- 38 A SKA was an account linked to a customer's DAB, which operated in a similar manner to a DAB. A SKA was sometimes used by customers to hold partial debt repayments owed to Crown (as described further below).

CVIs

- 39 Customers could use a number of different CVIs to obtain table 3, section 6 of the AML/CTF Act designated services from Crown Melbourne and Crown Perth. These included chips, chip exchange vouchers (**CEV**), TITOs, and CPVs.
- 40 Customers who did not have a DAB or SKA could buy-in at a table game using cash, or were able to purchase a CEV at the Cage, which could be exchanged for chips at a gaming table. During the Relevant Period, Crown offered non-Cage buy-in facilities, which enabled customers to purchase chips or vouchers for use at gaming tables. Between mid-2018 and mid-2021, Crown Melbourne also offered chip dispensing machines, which allowed patrons to exchange cash for chips.

Card Play, Card Play Extra and Cashless accounts

- 41 Crown Melbourne offered a Card Play account (also known as a Loyalty Crown Rewards Cashless Account), which was an account linked to a Crown Rewards card, and allowed customers playing on gaming machines to transfer funds from their DAB to their cards, or credits between their Crown Rewards cards and gaming machines (ie, deposit credits from gaming machines onto their Crown Rewards cards, or withdraw credits from their Crown Rewards cards to gaming machines). Credits could be cashed out by 'collecting' a ticket from a gaming machine and cashing that ticket out at the Cage (including depositing funds to their DAB) or at a ticket redemption terminal (**TRT**) (up to \$2,000 per transaction).
- 42 At Crown Melbourne, a Card Play Extra account was an extra functionality of the Card Play account, whereby customers had the ability to deposit and withdraw money to and from their Crown Rewards card at the Cage or at a TRT (up to \$2,000 per transaction), without having to collect a ticket from a gaming machine. Money on the card could otherwise only be used as credit for gaming machines. Money on Card Play Extra accounts could be withdrawn as cash at a TRT (up to \$2,000) or the Cage.
- 43 Crown Perth offered a 'Cashless' account, which provided customers who used this service with the same functionality as the Card Play Extra account provided to customers at Crown Melbourne. A Cashless account at Crown Perth was available only to Pearl Room members.
- 44 Gaming machines could also be played by inserting cash directly into the machine (with or without first inserting a membership card). Winnings were collected by the machine issuing a ticket for redemption at a TRT or the Cage.
- 45 Transactions on Card Play, Card Play Extra and Cashless accounts involved the provision of item 13, table 3, section 6 designated services.

² For example, as a chip purchase voucher (**CPV**) (which could be exchanged for chips at gaming tables) or TITO (which could be used to enable play on gaming machines).

Cheque Cashing Facility (CCF), Credit Facility / Funds Advance Facility (Credit Facility)

- 46 Customers were able to apply for a CCF, which was a facility at Crown under which a domestic or international customer could be advanced money. This advance of money was a 'loan' within the meaning of section 5 of the AML/CTF Act. A customer approved for a CCF entered into a CCF Agreement with Crown that provided for an agreed credit limit. 'Loans' within the meaning of section 5 of the AML/CTF Act were made by Crown through CCFs in the course of carrying on a loans business. Crown provided designated services under item 6, table 1, section 6 of the AML/CTF Act when it advanced money to a customer under a CCF.
- 47 A customer could transact on a CCF at the Cage up to the approved limit by requesting CPVs, gaming chips, cash or cash equivalent, or if the CCF was linked to a DAB, an amount to be credited to the customer's DAB. When the customer transacted in this way on the CCF, the customer either presented a personal cheque at the Cage or was issued with a counter cheque (known as a house cheque at Crown Perth) by the Cage that was made out up to an amount that was less than or equal to the approved facility limit. A customer could transact up to the face value of the cheque or cheques presented or issued at Crown Melbourne, Crown Perth or both (depending on the facility).
- 48 In order to transact on a CCF using the means set out in paragraph 47, the customer could either provide a personal cheque (although Crown did not accept all cheque types), or be issued with a bankable document called a 'counter cheque' or 'house' cheque' by Crown Melbourne or Crown Perth respectively.
- 49 A customer could repay a CCF by cash payment at the Cage, domestic or international telegraphic transfer to Crown Melbourne or Crown Perth (by the customer or, prior to November 2020 only, by a third party), applying gaming chips, CPVs or cash equivalents held by the customer, transferring funds from the customer's DAB or by setting-off the amount owing against the customer's winnings at Crown Melbourne or Crown Perth.
- 50 Where a customer transacted on a CCF by providing a personal cheque, the CCF would be repaid by Crown Melbourne or Crown Perth banking the cheque within a specified timeframe unless the funds owing were redeemed beforehand. Otherwise, a customer could redeem a personal cheque or a counter cheque / house cheque by any of the means set out in paragraph 49. Crown Melbourne and Crown Perth each had documented guidance setting out how to recover payments from customers in the event that a cheque was dishonoured.
- 51 By allowing a transaction in relation to a CCF (including by banking or redeeming a personal cheque, counter cheque or house cheque), Crown provided an item 7, table 1, section 6 designated service.
- 52 Crown also offered a Credit Facility, being a facility where an international customer could be advanced money. An advance of money under a Credit Facility was a 'loan' within the meaning of section 5 of the AML/CTF Act. A customer approved for a Credit Facility entered into a Credit Facility Agreement with Crown that provided for an agreed credit limit. 'Loans' within the meaning of section 5 of the AML/CTF Act were made by Crown through Credit Facilities in the course of carrying on a loans business. Crown provided designated services under item 6, table 1, section 6 of the Act when it advanced money to a customer under a Credit Facility.
- 53 A customer could transact on a Credit Facility up to the approved limit by requesting Credit Marker/s (a non-bankable instrument issued by Crown to a customer against the approved facility) for CPVs, gaming chips, cash or cash equivalent, or, if the facility was linked to a DAB,

an amount to be credited to the customer's DAB. At Crown Perth, this facility was known as a Funds Advance Facility and a Credit Marker was known as a Draw Down Marker. Crown Perth ceased providing Funds Advance Facilities on or around 23 February 2021.

- 54 A customer could redeem a Credit Marker (or repay any amount advanced by Crown) in a number of ways including by cash payment at the Cage, domestic or international telegraphic transfer to Crown Melbourne or Crown Perth (by the customer or, prior to November 2020 only, by a third party), applying gaming chips, CPVs or cash equivalents held by the customer, transferring funds from the customer's DAB or by setting-off the amount owing against the customer's winnings at Crown Melbourne or Crown Perth.
- 55 By allowing a transaction in relation to the Credit Facility (including by redeeming a Credit Marker) Crown provided an item 7, table 1, section 6 designated service.

Hotel Card channel

- 56 The Hotel Card channel operated at Crown Melbourne from approximately 2012 until October 2016. Customers could use debit or credit cards at the Crown Towers Hotel to authorise a transfer of funds to be made available to them at the Crown Melbourne casino. This involved the provision of item 32, table 1, section 6 designated services.

Overseas deposit services

- 57 Crown Melbourne and Crown Perth provided overseas deposit services to customers through:
- (a) the City of Dreams casinos in Macau until October 2016 and Manila until May 2017;
 - (b) Company 10, based in South East Asia, from at least 1 January 2015 until September 2020; and
 - (c) Crown Aspinalls in London until August 2019.
- 58 The overseas deposit services allowed a person to deposit funds at the overseas locations with the equivalent value being made available to a customer for use at Crown Melbourne or Crown Perth. The person depositing the funds did not need to be the same person as the customer. These services involved the provision of item 32, table 1, section 6 designated services by Crown Perth and Crown Melbourne.

Foreign currency exchange

- 59 Crown Melbourne and Crown Perth provided foreign currency exchange services to customers within the meaning of item 14, table 3, section 6 of the AML/CTF Act. Crown accepted physical currency, foreign drafts and travellers' cheques for the purposes of currency exchange. Customers could also deposit or transfer funds into foreign currency accounts held by Crown Melbourne and Crown Perth. Crown Melbourne and Crown Perth would convert the funds to Australian dollars and make them available to the customer in their DAB. Currency exchange was also facilitated for customers who were repaying debts owed to Crown Melbourne and Crown Perth.

Foreign currency services

- 60 Until March 2020, Crown Melbourne and Crown Perth provided, or had the capacity to provide, a number of designated services in Hong Kong Dollars (**HKD**), including gaming services to international players and the provision of chips and credit in HKD.

C.5 Turnover, revenue and profit

- 61 Certain transactions engaged in by customers with Crown Melbourne and Crown Perth during the Relevant Period were recorded as 'turnover'. Total turnover reflects the total amount wagered by customers. It includes the re-betting of winnings and, accordingly, can be many multiples of the buy-in³ and/or cash out⁴ of the customer. On each occasion that a customer wagers money on a game, a designated service under table 3, section 6 of the AML/CTF Act is provided. However, because of re-betting of winnings, turnover does not represent the total value of money brought into or moved through a casino by the customer.
- 62 However, turnover is relevant to quantifying the nature and scale of the ML/TF risks posed by junkets and high-risk customers. High turnover, including through complex transaction chains and within junkets, provides criminals with the opportunity to mix illicit funds with legitimate funds and to obscure the source of funds.⁵ High turnover increases the risk of ML/TF. Appropriate risk-based procedures, systems and controls are required to be included in AML/CTF Programs to address the ML/TF risks of high turnover through junket customers.⁶
- 63 Revenue from designated services provided through gaming channels (including junket channels) is a fraction of total turnover. Revenue is the aggregate of customer losses, after the aggregate of customer wins have been paid out.
- 64 As with any business, revenue in relation to certain customers or groups of customers is not instructive of the profit, if any, to Crown resulting from its dealings with those customers. Revenue figures do not take into account Crown's costs. Profits to Crown, if any, from particular customers or customer groups are very difficult to calculate, but will only ever represent a fraction of the revenue earned by Crown in relation to those customers.
- 65 The revenue and turnover figures referenced in this SAFA measure revenue and turnover generated by particular categories of customer during the Relevant Period, not revenue and turnover which would not have necessarily arisen had the contraventions admitted in this SAFA not occurred (the extent of which is not known).

C.6 Junkets

- 66 A junket is an arrangement between a casino and a junket operator that facilitates gambling by one or more high wealth players (ie, junket players) at the casino. Junket operators can be represented by one or more junket representatives.
- 67 Between 1 March 2016 and March 2020, Crown Melbourne and Crown Perth facilitated junket programs, ranging from junkets of just one junket player, to 'platform junkets', which were generally larger junkets featuring numerous players. For the purposes of the proceeding, it is relevant to note the five platform junkets that were operated by the following customers:
- (a) Customer 1, who operated a junket branded as the 'Suncity' junket (the **Suncity junket**) (see case study at G.1.1.1);
 - (b) Customer 2, who was the operator of the Song junket;
 - (c) Customer 3, who was the operator of the Meg-Star junket (see case study at G.1.1.2);

³ Buy-in refers to the purchase by a customer of chips or other CVIs.

⁴ Cash out refers to the exchange of chips or other CVIs for money.

⁵ See paragraph 13 for an explanation of complex transaction chains.

⁶ See paragraphs 15 to 17 for an explanation of appropriate risk-based procedures, systems and controls.

- (d) Person 3 and Customers 6 - 9, who formed a network of junket operators affiliated with the Neptune Group and Neptune Guangdong Group (the **Neptune junket**); and
 - (e) Customers 10 - 14, who were the junket operators affiliated with the Chinatown junket (the **Chinatown junket**).
- 68 The relationship between Crown Melbourne or Crown Perth and each junket operator was governed by an overarching 'non-exclusive gaming promotion agreement'. In addition, for each junket program, Crown Melbourne or Crown Perth and the junket operator (or authorised junket representative) entered into a Junket Program Agreement, which set out rebates and commissions payable to junket operators on the basis of wins/losses at the time of settlement (for rebates) and total turnover (for commissions).
- 69 From 1 March 2016 until March 2020, revenue from designated services provided through junket channels represented a material source of both Crown Melbourne's and Crown Perth's total revenues, as detailed in paragraph 349(h).
- 70 In August 2020, the Crown Resorts Board resolved that the Crown Group would cease dealing with junkets on a temporary basis. In November 2020, the Crown Resorts Board permanently banned junkets.
- 71 The provision of designated services to customers through junkets involved higher ML/TF risks than services provided through other channels because:
- (a) junket operators and representatives facilitated the provision of certain designated services to junket players, often in high values;
 - (b) junket programs often involved the movement of large amounts of money across borders, and, depending on the specific junket program, may have involved the use of multiple bank accounts, including by third parties, which could obscure the identities of persons conducting the transactions through junket programs and the source and ownership of funds of customers;
 - (c) on a per-transaction and per-customer basis, the junket tour operations sector was exposed to the risks associated with high-value cash activity;
 - (d) junket operators used formal or informal systems to remit money;
 - (e) inherent to the junket tour operators sector was exposure to some higher ML/TF risk jurisdictions. In particular, there were vulnerabilities associated with jurisdictions with currency flight and gambling restrictions in place as these measures could create demand for covert money remittances which could be exploited by criminal groups. In addition, having a customer base composed of predominantly foreign residents could increase the junket sector's attractiveness and exposure to transnational serious and organised crime, and could mean that the source and designation of funds, and information about customers' criminal and financial activity, were difficult to identify as the customers were located in foreign jurisdictions;
 - (f) junket players generally relied on the junket operators to make their funds available at the casinos, including through Credit Facilities;
 - (g) there could be a lack of transparency and level of anonymity by the long and complex value chains associated with the flows of junket-related funds, the pooling of all players' funds and transactions under the name of the junket operator, and the provision of cash

to players in circumstances where the source of funds and purpose for which the cash was used may be unknown;

- (h) the financial arrangements between junket operators and junket players were not disclosed to Crown;
- (i) the features of junkets could create layers of obscurity around the identities of persons conducting transactions through junket programs and the source and ownership of funds of customers, particularly if they were located in foreign jurisdictions;
- (j) junket programs could be vulnerable to cuckoo smurfing and structuring; and
- (k) money deposited with a junket account and then subsequently withdrawn with minimal gaming activity could give the funds the appearance of legitimacy. In addition, any 'parking' of illicit money put distance between the act or acts that generated the illicit funds and the ultimate recipients of those funds, making it harder to trace the flow of money.

D. RELEVANT OBLIGATIONS UNDER THE AML/CTF ACT

- 72 Throughout the Relevant Period, section 36(1) of the AML/CTF Act required a reporting entity to monitor the reporting entity's customers in relation to the provision of designated services, with a view to identifying, mitigating and managing ML/TF risk. This monitoring had to be conducted in accordance with the AML/CTF Rules, including the requirements set out in Chapter 15 (described at paragraph 78 below).
- 73 Throughout the Relevant Period, section 81 of the AML/CTF Act stated 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 AML/CTF program within the meaning of section 83 of the AML/CTF Act that applies to the reporting entity (being either a standard, joint or special AML/CTF program).
- 74 The AML/CTF program is the principal document for setting out the risk-based systems and controls that are required to ensure compliance with the AML/CTF Act and the AML/CTF Rules. It is the means through which a reporting entity is required to take responsibility for managing the ML/TF risks of its own business.
- 75 Throughout the Relevant Period:
- (a) section 84(1) of the AML/CTF Act defined a standard AML/CTF program as a written program that applies to a particular reporting entity, and is divided into the following parts: Part A (general) and Part B (customer identification); and
 - (b) section 85(1) of the AML/CTF Act defined a joint AML/CTF program as a written program that applies to each reporting entity that from time to time belongs to a particular designated business group (**DBG**), and is divided into the following parts: Part A (general) and Part B (customer identification).

Part A of an AML/CTF program

- 76 Throughout the Relevant Period, sections 84(2) and 85(2) of the AML/CTF Act defined Part A of a standard or joint AML/CTF program (**Part A Program**) as a part which:
- (a) has the primary purpose of identifying, mitigating and managing the risk that a reporting entity may reasonably face that the provision of designated services at or through a

permanent establishment of the reporting entity in Australia might (whether inadvertently or otherwise) involve or facilitate ML/TF; and

- (b) complies with such requirements as are specified in the AML/CTF Rules (s 84(2)(c) of the AML/CTF Act).

The Part A Program's primary purpose of identifying, mitigating and managing ML/TF risks

77 With respect to paragraph 76(a), a reporting entity's Part A Program will not have the primary purpose of identifying, mitigating and managing ML/TF risks reasonably faced if the Part A Program:

- (a) does not refer to or incorporate a written ML/TF risk assessment methodology that is capable of appropriately identifying and assessing the ML/TF risks of all designated services provided by a reporting entity;
- (b) is not aligned to the ML/TF risks reasonably faced by the reporting entity with respect to designated services, as periodically assessed in accordance with an appropriate ML/TF risk assessment methodology;
- (c) does not include or establish an appropriate framework for approval and oversight by Board and senior management: see paragraph 135; and
- (d) does not include appropriate risk-based systems and controls that are capable (as a matter of system or control design) of identifying, mitigating and managing ML/TF risks reasonably faced by the reporting entity, consistent with risk appetite.⁷

The requirements of the AML/CTF Rules relating to AML/CTF Programs

78 With respect to paragraph 76(b), the relevant AML/CTF Rules included, but were not limited to:

- (a) paragraphs 8.1.3 (for a Standard Part A Program) and 9.1.3 (for a Joint Part A Program), which provided that, in determining and putting in place appropriate risk-based systems and controls, a Part A Program must have regard to the following factors in relation to the reporting entity (for a Standard Part A Program) or each reporting entity in the DBG (for a Joint Part A Program):
 - (i) the nature, size and complexity of business; and
 - (ii) the type of ML/TF risk that might reasonably be faced;
- (b) paragraphs 8.1.4 (for a Standard Part A Program) and 9.1.4 (for a Joint Part A Program), which provided that, for the purposes of the relevant AML/CTF Rules, in identifying the ML/TF risk, a Part A Program must take account of the risk posed by the following factors in relation to the reporting entity (for a Standard Part A Program) or each reporting entity in the DBG (for a Joint Part A Program):
 - (i) the customer types, including any PEPs;
 - (ii) the types of designated services provided;
 - (iii) the methods by which designated services are delivered; and
 - (iv) the foreign jurisdictions dealt with;

⁷ See paragraphs 15 to 17 for an explanation of appropriate risk-based procedures, systems and controls.

- (c) paragraphs 8.1.5 (for a Standard Part A Program) and 9.1.5 (for a Joint Part A Program), which provided that a Part A Program must be designed to enable the reporting entity (for a Standard Part A Program) or each reporting entity in the DBG (for a Joint Part A Program) to:
 - (i) understand the nature and purpose of the business relationship with its customer types, including, as appropriate, the collection of information relevant to that understanding;
 - (ii) understand the control structure of non-individual customers;
 - (iii) identify significant changes in ML/TF risk for the purposes of its AML/CTF program (Part A and Part B), including:
 - (A) risks identified by consideration of the factors in paragraphs 8.1.4 and 9.1.4 (see sub-paragraph (b) above); and
 - (B) risks arising from changes in the nature of the business relationship, control structure or beneficial ownership of its customers; and
 - (iv) recognise such changes in ML/TF risk for the purposes of the requirements of its AML/CTF program (Part A and Part B); and
 - (v) identify, mitigate and manage any ML/TF risk arising from:
 - (A) all new designated services prior to introducing them to the market;
 - (B) all new methods of designated service delivery prior to adopting them;
 - (C) all new or developing technologies used for the provision of a designated service prior to adopting them; and
 - (D) changes arising in the nature of the business relationship, control structure or beneficial ownership of its customers;
- (d) parts 8.2 (for a Standard Part A Program) and 9.2 (for a Joint Part A Program), which provided that a Part A Program must include an AML/CTF risk awareness training program that satisfies the requirements in parts 8.2 (for a Standard Part A Program) and 9.2 (for a Joint Part A Program);
- (e) parts 8.4 (for a Standard Part A Program) and 9.4 (for a Joint Part A Program), which provided that a Part A Program must be approved by and subject to the ongoing oversight of:
 - (i) for a Standard Part A Program, the reporting entity's governing board and senior management; and
 - (ii) for a Joint Part A Program, the governing board and senior management of each reporting entity in the DBG, or where each member of the DBG is related to the other members, the governing board and senior management of the main holding company of the group;
- (f) paragraphs 8.5.1 (for a Standard Part A Program) and 9.5.1 (for a Joint Part A Program), which provided that a Part A Program must provide for the reporting entity (for a Standard Part A Program) or the DBG (for a Joint Part A Program) to designate a person as the 'AML/CTF Compliance Officer' at management level;

- (g) parts 8.6 (for a Standard Part A Program) and 9.6 (for a Joint Part A Program), which provided that a Part A Program must be subject to regular independent review;
- (h) parts 8.7 (for a Standard Part A Program) and 9.7 (for a Joint Part A Program), which provided that a reporting entity must take into account any applicable guidance material disseminated or published by AUSTRAC and any feedback provided by AUSTRAC in respect of the relevant reporting entity or the industry it operates in that is relevant to the identification, mitigation and management of ML/TF risk;
- (i) paragraphs 8.9.1(2) (for a Standard Part A Program) and 9.9.1(2) (for a Joint Part A Program), which provided that a Part A Program must include appropriate systems and controls designed to ensure compliance with the reporting entity's reporting obligations under sections 41 (relating to suspicious matter reports (**SMRs**)), 43 (relating to threshold transaction reports (**TTRs**)) and 45 (relating to international funds transfer instructions (**IFTIs**)) of the AML/CTF Act;
- (j) paragraph 15.2, which provided that a Part A Program must include appropriate risk-based systems and controls to enable the reporting entity to determine in what circumstances further 'know your customer' (**KYC**) information or beneficial owner information should be collected or verified, to enable the review and update of KYC information and beneficial owner information for OCDD purposes;
- (k) paragraph 15.3, which required a reporting entity to undertake reasonable measures to keep, update and review the documents, data or information collected under the applicable customer identification procedure (particularly in relation to high risk customers) and the beneficial owner identification requirements specified in Chapter 4 of the AML/CTF Rules;
- (l) paragraphs 15.4 to 15.7, which provided that a Part A Program must include a transaction monitoring program (**TMP**) that:
 - (i) includes appropriate risk-based systems and controls to monitor the transactions of customers;
 - (ii) has the purpose of identifying, having regard to ML/TF risk, any transaction that appears to be suspicious within the terms of section 41 of the AML/CTF Act; and
 - (iii) has regard to complex, unusual large transactions and unusual patterns of transactions which have no apparent economic or visible lawful purpose;
- (m) paragraphs 15.8 and 15.9, which provided that a Part A Program must include an enhanced customer due diligence program (**ECDD Program**), which is applied by the reporting entity (subject to paragraph 4.4.18 of the AML/CTF Rules) when:
 - (i) it determines under its risk-based systems and controls that the ML/TF risk is high;
 - (ii) a designated service is being provided to a customer who is or who has a beneficial owner who is a foreign PEP;
 - (iii) a suspicion has arisen for the purposes of section 41 of the AML/CTF Act; or
 - (iv) the reporting entity is entering into or proposing to enter into a transaction and a party to the transaction is physically present in, or is a corporation incorporated in, a prescribed foreign country;

- (n) paragraph 15.10, which provided that the ECDD Program must include appropriate risk-based systems and controls so that, in cases where one or more of the circumstances in paragraph 15.9 arises, the reporting entity undertakes measures appropriate to those circumstances, including, but not limited to:
 - (i) undertaking more detailed analysis of the customer's KYC information and beneficial owner information, including, where appropriate, taking reasonable measures to identify the customer and each beneficial owner's source of wealth and source of funds; and
 - (ii) seeking senior management approval for continuing a business relationship with the customer, and whether a designated service should continue to be provided to the customer; and
- (o) paragraph 15.11, which provided that where the customer is a foreign PEP, or has a beneficial owner who is a foreign PEP, the measures at paragraph 78(n) above must be undertaken at a minimum.

Part B of an AML/CTF program

- 79 Throughout the Relevant Period, sections 84(3) and 85(3) of the AML/CTF Act defined Part B of a standard or joint AML/CTF program (**Part B Program**) as a part which:
- (a) has the sole or primary purpose of setting out the customer identification procedures applicable to customers of the reporting entity (**ACIPs**); and
 - (b) complies with any such requirements as are specified in the AML/CTF Rules.
- 80 With respect to paragraph 79(b), the relevant AML/CTF Rules included, but were not limited to:
- (a) paragraph 4.2.2, which provided that an AML/CTF program must include appropriate risk-based systems and controls that are designed to enable the reporting entity to be reasonably satisfied, where a customer is an individual, that the customer is the individual that he or she claims to be;
 - (b) paragraph 4.2.3, which provided that an AML/CTF program must include a procedure for the reporting entity to collect, at a minimum, the name, date of birth and residential address of a customer that is an individual (**Minimum KYC Information**);
 - (c) paragraph 4.2.5, which provided that an AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to determine whether, in addition to the KYC information referred to in paragraphs 4.2.3 or 4.2.4, any other KYC information will be collected about a customer;
 - (d) paragraph 4.2.6, which provided that an AML/CTF program must include a procedure for the reporting entity to verify, at a minimum, a customer's full name, and either the customer's date of birth or residential address;
 - (e) paragraph 4.2.8, which provided that an AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to determine whether, in addition to the KYC information referred to in paragraph 4.2.6, any other KYC information collected about a customer should be verified from reliable and independent documentation, reliable and independent electronic data or a combination of the two;

- (f) paragraphs 4.11.1 to 4.11.4, which provided requirements relating to the collection and verification of documents and information in circumstances where an agent is acting on behalf of a customer that is an individual; and
- (g) paragraphs 4.13.1 to 4.13.4, which provided requirements relating to PEPs.

E. CROWN MELBOURNE'S AND CROWN PERTH'S AML/CTF PROGRAMS

E.1 Crown Melbourne Standard Program

- 81 Between 1 March 2016 and 1 November 2020, Crown Melbourne had a standard AML/CTF program, which included a document titled 'Crown Melbourne Limited Anti-Money Laundering / Counter-Terrorism Financing Program'. This document was updated over time and relevantly comprised the following versions:
- (a) Version 7.0 effective from 2 February 2016 to 18 January 2017;
 - (b) Version 7.1 effective from 19 January 2017 to 26 November 2018; and
 - (c) Version 8.0 effective from 27 November 2018 to 1 November 2020,
- (each, the **Crown Melbourne Standard Program**).
- 82 The Crown Melbourne Standard Program included sections addressing the following matters:
- (a) program management, including in relation to approval, amendment and oversight of the program (clause 3 and Annexure A of the Crown Melbourne Standard Program);
 - (b) independent review of the program (clause 4 and Annexure B of the Crown Melbourne Standard Program);
 - (c) employee due diligence (clause 5 and Annexure C of the Crown Melbourne Standard Program);
 - (d) AML/CTF risk awareness training (clause 6 and Annexure D of the Crown Melbourne Standard Program);
 - (e) risk assessments for existing and proposed new casino designated services (clauses 7 and 8 and Annexures E and J of the Crown Melbourne Standard Program);
 - (f) Crown Melbourne's relationship with AUSTRAC, including processes for incorporating AUSTRAC guidance in the Crown Melbourne Standard Program (clause 9 of the Crown Melbourne Standard Program);
 - (g) record-keeping (clause 10 of the Crown Melbourne Standard Program);
 - (h) transaction monitoring, including descriptions of the kinds of transactions to be monitored and processes relating to reporting obligations (clauses 12 and 19 and Annexure F of the Crown Melbourne Standard Program);
 - (i) customer risk ratings and exclusion of high risk customers (clauses 13 and 16 and Annexure G of the Crown Melbourne Standard Program);
 - (j) the collection of KYC information and the conduct of enhanced customer due diligence (**ECDD**) (clauses 14 and 15 and Annexures H and I of the Crown Melbourne Standard Program);
 - (k) the identification of PEPs (clause 17 of the Crown Melbourne Standard Program);

- (l) the treatment of non-individual customers (clause 18 and Annexures I and K of the Crown Melbourne Standard Program); and
- (m) customer identification, verification and re-verification (clauses 20 to 24 and Annexures I and K of the Crown Melbourne Standard Program).

83 The Crown Melbourne Standard Program was supported by a number of policies and procedures, including the 'AUSTRAC Guidelines' (later referred to as the 'AML/CTF Act and AML/CTF Rules Compliance Guidelines'), which were intended to provide information to employees of Crown Melbourne to assist with compliance with the Crown Melbourne Standard Program and with the AML/CTF Act and AML/CTF Rules generally. This document was updated over time and relevantly comprised the following versions:

- (a) 'AUSTRAC Guidelines', version 5.0, effective from 31 October 2014 to 5 May 2016;
- (b) 'AUSTRAC Guidelines', version 6.0, effective from 6 May 2016 to April 2017;
- (c) 'AUSTRAC Guidelines', version 6.1, effective from April 2017 to July 2018; and
- (d) 'AML/CTF Act and AML/CTF Rules Compliance Guidelines', version 7.0, effective from July 2018 to 1 November 2020,

(each, the **Crown Melbourne Guidelines**).

E.2 Crown Perth Standard Program

84 Between 1 March 2016 and 1 November 2020, Crown Perth had a standard AML/CTF program, which included a document titled 'Crown Perth AML/CTF Program'. This document was updated over time and relevantly comprised the following versions:

- (a) Version 14 effective from 28 April 2015 to 13 December 2016;
- (b) Version 15 effective from 14 December 2016 to 23 April 2017;
- (c) Version 16 effective from 24 April 2017 to 2 December 2018; and
- (d) Version 17 effective from 3 December 2018 to 1 November 2020,

(each, the **Crown Perth Standard Program**).

85 The Crown Perth Standard Program included sections addressing the following matters:

- (a) program management, including in relation to approval, amendment and oversight of the program (clause 3 of the Crown Perth Standard Program);
- (b) independent review of the program (clause 4 and Appendix D of the Crown Perth Standard Program);
- (c) employee due diligence (clause 5 of the Crown Perth Standard Program);
- (d) AML/CTF risk awareness training (clause 6 and Appendix C of the Crown Perth Standard Program);
- (e) risk assessments for existing and proposed new casino designated services (clauses 7 and 8 and Appendices E and H of the Crown Perth Standard Program);
- (f) Crown Perth's relationship with AUSTRAC, including processes for incorporating AUSTRAC guidance in the Crown Perth Standard Program (clause 9 of the Crown Perth Standard Program);
- (g) record-keeping (clause 10 of the Crown Perth Standard Program);

- (h) transaction monitoring, including descriptions of the kinds of transactions to be monitored (clause 12 of the Crown Perth Standard Program);
- (i) customer risk ratings and exclusion of high risk customers (clauses 13 and 16 and Appendices A and B of the Crown Perth Standard Program);
- (j) the collection of KYC information and the conduct of ECDD (clauses 14 and 15 and Appendices A, B, F and G of the Crown Perth Standard Program);
- (k) reporting obligations (clause 17 of the Crown Perth Standard Program); and
- (l) customer identification, verification and re-verification (clauses 18 to 20 and Appendices A, B, F and G of the Crown Perth Standard Program).

86 The Crown Perth Standard Program was supported by a number of policies and procedures, including the 'Legal Services – AML Standard Operating Procedures', which set out the operational procedures to be followed by the Legal Officer – AML (or designee) with respect to the Crown Perth Standard Program. This document was updated over time and relevantly comprised the following versions:

- (a) Version 11 effective from 1 October 2015 to 30 September 2016;
- (b) Version 12 effective from 1 October 2016 to 31 January 2017;
- (c) Version 13 effective from 1 February 2017 to 31 March 2017;
- (d) Version 14 effective from 1 April 2017 to 1 November 2018; and
- (e) Version 15 effective from 2 November 2018 until November 2020, when the Joint AML/CTF Policy and Procedures was adopted,

(the **Crown Perth AML SOPs**).

E.3 Crown Joint AML/CTF Program

87 Since 2 November 2020, Crown Melbourne and Crown Perth have adopted a joint AML/CTF program, which has comprised the following documents during the Relevant Period:

- (a) 'Crown Resorts Limited Joint Anti-Money Laundering & Counter-Terrorism Financing Program Part A':
 - (i) Version 2.0 effective from 2 November 2020 to 30 January 2022; and
 - (ii) Version 3.0 effective from 31 January 2022;
- (b) 'Crown Resorts Limited Joint Anti-Money Laundering & Counter-Terrorism Financing Program Part B':
 - (i) Version 2.0 effective from 2 November 2020 to 9 August 2021; and
 - (ii) Version 2.1 effective from 10 August 2021;
- (c) 'Crown Resorts Limited Joint Anti-Money Laundering and Counter-Terrorism Financing Policy and Procedures':
 - (i) Version 1.0, effective from 2 November 2020 to 28 September 2021; and
 - (ii) Version 2.0, effective from 29 September 2021 to 31 January 2022 (when the Crown Resorts Limited Joint Anti-Money Laundering and Counter-Terrorism Financing Policy and Procedures was incorporated into version 3.0 of the Crown

F. CROWN'S CONTRAVENTIONS OF SECTION 81 OF THE AML/CTF ACT – STANDARD AND JOINT PROGRAMS

F.1 Risk assessments

88 To comply with the provisions described in Section D, a Standard or Joint Part A Program must, among other things:

- (a) refer to or incorporate an appropriate written ML/TF risk assessment methodology that is capable of appropriately identifying and assessing the ML/TF risks of the designated services provided by the reporting entity;
- (b) be based on, and aligned to, a ML/TF risk assessment (or risk assessments) that:
 - (i) address the matters in paragraphs 8.1.3 and 8.1.4 (for Standard Programs) or paragraphs 9.1.3 and 9.1.4 (for Joint Programs) of the AML/CTF Rules; and
 - (ii) is conducted in accordance with a written risk assessment methodology as described in sub-paragraph (a) above; and
- (c) include appropriate procedures that enable the identification, assessment and recognition of the matters listed in paragraph 8.1.5 (for Standard Programs) or paragraph 9.1.5 (for Joint Programs) of the AML/CTF Rules.⁸

89 At no time during the Relevant Period did Part A of the Crown Melbourne Standard Program or Part A of the Crown Perth Standard Program (together, the **Standard Part A Programs**):

- (a) refer to or incorporate an appropriate written ML/TF risk methodology to assess the inherent ML/TF risks of designated services, having regard to paragraphs 8.1.3 and 8.1.4 of the AML/CTF Rules;
- (b) refer to or incorporate an appropriate written risk assessment methodology to assess the residual ML/TF risks⁹ of designated services, once risk-based controls had been applied; or
- (c) include appropriate procedures for the identification, assessment and management of the matters listed in paragraph 8.1.5 of the AML/CTF Rules.

90 As a result, the Standard Part A Programs during the Relevant Period were not aligned to the ML/TF risks reasonably faced by Crown and were not capable (as a matter of control or systems design) of identifying, mitigating and managing these risks contrary to sections 84(2)(a) and (c) of the AML/CTF Act. The reasons are set out at paragraphs 91 to 122.

F.1.1 Crown's Risk Registers

91 From 1 March 2016 to 1 November 2020, Appendix E of the Standard Part A Programs included a register of ML/TF risks (**Risk Register**). The systems and controls provided for in the Crown Perth Standard Program and the Crown Melbourne Standard Program purported to address the ML/TF risks identified in their respective Risk Registers.

⁸ See paragraphs 15 to 17 for an explanation of appropriate procedures, systems and controls.

⁹ A residual risk is the risk that remains after risk procedures, systems and controls are applied to the inherent risk.

- 92 Annexure E of the Crown Melbourne Standard Program and the Crown Perth Standard Program required the Risk Register to be updated annually.

Overview

- 93 Each Risk Register:
- (a) included a description of some of the designated services provided by Crown Perth or Crown Melbourne (as applicable), the technologies used to deliver those designated services, and some ML/TF risks identified as being associated with those designated services;
 - (b) intended to address the inherent ML/TF risk associated with each designated service;
 - (c) listed controls in place intended to address the inherent ML/TF risks identified; and
 - (d) intended to calculate the residual ML/TF risk associated with designated services after controls had been applied.
- 94 Each time a Risk Register was completed, Crown Melbourne and Crown Perth assessed its residual ML/TF risk to be low.
- 95 The completion of the Risk Register was not conducted pursuant to a documented methodology that:
- (a) covered all relevant inherent risks and associated risk attributes reasonably faced by Crown Melbourne and Crown Perth with respect to the designated services they provided and had appropriate regard to the nature, size and complexity of the Crown Melbourne and Crown Perth businesses;
 - (b) appropriately considered the ML/TF risk factors of customer, channel and jurisdiction; and
 - (c) appropriately assessed the residual ML/TF risks of designated services, once risk-based controls had been applied.¹⁰

Risks associated with designated services

- 96 The Risk Registers identified and assessed some ML/TF risks in relation to a number of designated services provided by Crown. However, the Risk Registers did not identify and assess all known ML/TF risks, typologies or vulnerabilities associated with the casino sector and with Crown Melbourne's and Crown Perth's business during the Relevant Period, including:
- (a) the different ML/TF risks posed by a number of different products or designated service types;
 - (b) cuckoo smurfing;
 - (c) offsetting;
 - (d) customers attempting to deposit front money or make payments using complex means;
 - (e) customers requesting transfers to and from other casinos; and
 - (f) loan sharking.¹¹

¹⁰ See paragraphs 15 to 17 for an explanation of appropriate procedures, systems and controls; see also the factors that an appropriate risk assessment must have regard to at paragraph 88.

¹¹ See Schedule 2 and paragraph 13.

97 Further, although they were considered to an extent in versions of the Standard Part A Programs, the Risk Registers did not articulate all known ML/TF typologies or vulnerabilities associated with:

- (a) the involvement of third parties in relation to customer transactions;
- (b) dramatic increases in gaming activity, including escalating risks of high turnover or high losses; and
- (c) misuse of certain CVIs.

Risks associated with customer types

98 The Risk Registers and the Standard Part A Programs did not categorise and rate the risks associated with all customer types or categories, including PEPs, high spenders, and customers the subject of law enforcement enquiries.

Risks associated with method of delivery of designated services (channels)

99 While the Risk Registers identified some ML/TF risks associated with certain designated services that were not provided via a face-to-face channel, during the Relevant Period the Registers and the Standard Part A Programs did not clearly identify the following activities as channels through which designated services were provided:

- (a) private gaming rooms;
- (b) Hotel Card channel (see section C.4 and paragraph 56, section F.3.5, and paragraphs 187(f) and 189(e));
- (c) junkets (see sections C.6 and F.5); and
- (d) Crown Patron Accounts (see sections C.4, F.4.1, F.4.2).

100 At no time during the period 1 March 2016 to 1 November 2020 did Crown Melbourne or Crown Perth otherwise assess the ML/TF risks posed by these channels, all of which gave rise to high inherent ML/TF risks.

101 The Risk Registers and the Standard Part A Programs did not recognise that some designated services (such as the Crown Patron Account channel) were not provided face-to-face, and did not assess the ML/TF risk associated with this feature.

Risks associated with jurisdiction

102 The Risk Registers and the Standard Part A Programs:

- (a) did not identify all the foreign jurisdictions that Crown dealt with;
- (b) inappropriately rated all jurisdictions as posing a 'low' ML/TF risk by default save for certain limited exceptions;
- (c) did not include or refer to procedures setting out when a consideration of jurisdiction would occur for the purposes of the Part A Programs; and
- (d) did not identify how jurisdictional risks were factored into the assessment of ML/TF risks of customer profiles, designated services and channels.

Holistic risk associated with designated services

- 103 The Risk Registers and the Standard Part A Programs did not appropriately assess the ML/TF risks reasonably faced by Crown with respect to the complexity of the designated services chains provided, as described in paragraph 13.

Controls

- 104 While the Risk Registers identified some controls, in the absence of an appropriate ML/TF risk assessment, these controls were not appropriately aligned or proportionate to the ML/TF risks faced by Crown Melbourne and Crown Perth. Further, the Risk Registers did not contain appropriate guidance to enable Crown to assess the design and operating effectiveness of the controls in mitigating and managing the identified ML/TF risks. Consequently, there was no documented justification for concluding in the Risk Registers that the residual ML/TF risk posed to each of Crown Melbourne and Crown Perth was low. The controls listed in the Risk Register did not reduce Crown's residual risk to low.¹²

F.1.2 Customer risk assessment

Methodology for assessing ML/TF risk posed by each customer

- 105 The Standard Part A Programs included the following framework to rate the ML/TF risk posed by each customer:
- (a) Clause 13 of the Standard Part A Programs stated that all Crown customers were automatically rated as presenting a 'low' ML/TF risk by default, unless the Standard Part A Programs or a decision made under them required otherwise.
 - (b) Annexure G of the Crown Melbourne Standard Program required the following types of customers to be automatically rated 'high' risk:
 - (i) customers known to have engaged in ML/TF;
 - (ii) customers known to be a foreign PEP;
 - (iii) companies; and
 - (iv) customers reviewed by the Persons of Interest (**POI**) Committee.
 - (c) Annexure G in each version of the Crown Melbourne Standard Program also identified trigger events for recording a risk rating higher than 'low'.
 - (d) Appendix B of the Crown Perth Standard Program required customers known to have engaged in ML/TF to be given an automatic 'high' ML/TF risk rating, with other criteria listed as prompting a review by the Ratings Officer to determine whether the customer's risk rating should be changed.
- 106 The Cash Transaction Reports Manager (**CTRM**) in Melbourne (from November 2018, the AML Team) and the Anti-Money Laundering Compliance Officer (**AMLCO**)/Ratings Officer in Perth were primarily responsible for determining whether to conduct assessments of customer risk ratings following a trigger event and whether to change a customer's risk rating.
- 107 The Standard Part A Programs did not include or incorporate appropriate guidance or criteria for identifying customers who may not have been low risk:

¹² See paragraphs 15 to 17 for an explanation of appropriate risk-based procedures, systems and controls.

- (a) The Standard Part A Programs did not include any guidance or criteria on assessing the ML/TF risks of customers with respect to table 1, section 6 of the AML/CTF Act financial services, including with respect to remittance services.
- (b) More broadly, the Standard Part A Programs contained limited guidance on what triggers must lead to a change in risk rating, largely leaving it to the discretion of the persons listed in paragraph 106 above.
- (c) The credit risk team carried out assessments of the credit risks posed by some international players and junkets visiting Crown Melbourne and Crown Perth. These credit risk assessments were not subject to any guidance or criteria relevant to ML/TF risks.
- (d) By no later than June 2018, the Chief Legal Officer of Crown Resorts, who was also the AMLCO for both Crown Melbourne and Crown Perth, was advised by the Group General Manager AML (Crown Melbourne) that the assessment and analysis of customer risk by Crown Melbourne was arbitrary and not subject to any concrete risk parameters.

Procedures for identifying and escalating potentially higher risk customers

- 108 There were no procedures in the Standard Part A Programs to consistently identify and escalate potentially higher risk customers (including PEPs) to the CTRM or AMLCO/Ratings Officer for assessment:
- (a) The Standard Part A Programs did not include written procedures to identify and escalate customers who were required to be rated as high risk under Crown Melbourne's and Crown Perth's own criteria. While, Annexure G of the Crown Melbourne Standard Part A Program and Appendices A and B of the Crown Perth Standard Part A Program identified categories of customers who posed higher ML/TF risks, the Standard Part A Program did not include procedures to consistently identify and escalate customers in these categories.
 - (b) Prior to 1 December 2018, Crown Melbourne screened all active customers with a significant or high risk rating through World-Check three times a week. An active customer was a customer who had activity noted against their account or Crown Rewards membership at a Crown entity within the previous 30 days. This process, by definition, was not applied to customers who were considered low risk by default.
 - (c) Prior to 1 December 2018, Crown Perth completed a report from FicroSoft data search system for any person listed in World-Check as a terrorist, criminal or PEP.
 - (d) From 1 December 2018, Crown Melbourne and Crown Perth ran a daily screen of all new customers, any existing customers who had updated their KYC information and all active customers through Dow Jones Risk and Compliance database. This was a consolidated list which was run across customers of both Crown Melbourne and Crown Perth.
 - (e) The Crown Perth Standard Program also required a World-Check on applications for deposit and credit facilities, on individual players on a junket program, customers on a premium program, or customers who were recorded as incoming international business to the Pearl Room.
 - (f) At all times, the CTRM or AML team in Melbourne or the Legal Officer, AML in Perth was required to manually review screening results to identify customers who may have required an active risk assessment. This review process was not adequately resourced.

Screening was conducted against customer data on SYCO. Customer information entered on SYCO was not always reliable.

- 109 For the period from 1 July 2020 to 30 June 2021, only 3.7% of carded Crown Melbourne and Crown Perth customers had been assigned a proactive risk rating, with the balance initially deemed to be 'low' or 'standard' risk by default, under Crown's customer risk ratings methodology during that time ('standard' risk replacing the term 'low' risk on and from 2 November 2020).
- 110 The Standard Part A Programs did not include or incorporate appropriate risk-based procedures to collect and analyse appropriate KYC information for the purposes of assessing a customer's risk at the stage of onboarding the customer, including with respect to source of wealth or source of funds:
- (a) Whilst Crown requested occupation information from customers in accordance with the Standard Part A Programs, it was optional for the customer to provide this. In the absence of a risk-based requirement in the Standard Part A Programs to obtain and assess information about source of wealth/funds (such as occupation) including for higher risk customer categories such as international VIP customers, Crown was unable to understand sufficiently the risk posed by certain customers.
 - (b) The Standard Part A Programs did not include appropriate risk-based processes to update, collect or verify further KYC information relating to the beneficial ownership of funds or the beneficiaries of transactions being facilitated, including the destination of funds.
- 111 The Standard Part A Programs included some risk-based procedures to collect and analyse further KYC information upon certain triggers, but these were not effective for the following reasons:
- (a) Clauses 14 and 22 in each version of the Crown Melbourne Standard Program and clauses 14, 15, and 20 in each version of the Crown Perth Standard Program provided that the CTRM should endeavour to obtain further KYC information from identified 'Significant Risk' or 'High Risk' customers or where, while conducting verification, a staff member suspected on reasonable grounds that the customer was not who he or she claimed to be. However, as Crown customers were low risk by default, and as procedures to identify and escalate customers who were not low risk by default were not appropriate (paragraph 108 and 109), these procedures were not effective.
 - (b) Annexure G of the Crown Melbourne Standard Program also required reasonable measures to be undertaken to establish the source of funds or source of wealth for any customer or beneficial owner identified by Crown as high risk and who was known to be a PEP or for any customer that was a company. As the Standard Part A Program did not include procedures to consistently identify and escalate customers who were high risk or PEPs (paragraph 108), these procedures were not effective.
 - (c) Annexure H of the Crown Melbourne Standard Program set out the ECDD measures to be taken as appropriate to the identified ML/TF risk. These measures required Crown staff to search for additional information about the customer, including clarifying or updating KYC information and seeking source of funds, source of wealth and beneficial ownership information. However, for the reasons set out at paragraph 257, these procedures were not appropriately risk-based.

- 112 The Standard Part A Programs did not include or incorporate any assurance processes relating to the methodology to assign risk ratings to customers.
- 113 The Standard Part A Programs did not include or incorporate appropriate information management systems with respect to the ML/TF risk posed by customers (see paragraphs 243(c) and 260). As a result, the Standard Part A Programs (as a matter of system or control design) were unable to appropriately identify, escalate and manage customers who posed higher ML/TF risks.

F.1.3 Identification and assessment of changing and emerging ML/TF risks

- 114 As the Standard Part A Programs were not based on and did not refer to or incorporate an appropriate written ML/TF risk assessment methodology, ML/TF risks were not capable of being consistently assessed and re-assessed over time. Accordingly, the Standard Part A Programs were not appropriately designed to enable Crown Melbourne and Crown Perth to identify significant changes in ML/TF risk and to recognise such changes in their Part A and Part B programs, contrary to paragraphs 8.1.5(3) and (4) of the AML/CTF Rules. Nor was Crown able to maintain Part A Programs that were capable, over time, of having the primary purpose of identifying, mitigating and managing ML/TF risks.
- 115 The Risk Registers were required to be reviewed annually. As the Risk Register did not include some of the key ML/TF risks reasonably faced by Crown Melbourne and Crown Perth with respect to all designated services, annual reviews were not capable of identifying significant changes in those ML/TF risks not identified by Crown and recognising such changes for the purposes of the Standard Part A and Standard Part B Programs, as required by paragraphs 8.1.5(3) and (4) of the AML/CTF Rules.
- 116 In addition to annual updates to the Risk Register, the Standard Part A Programs also included the following mechanisms to identify and assess changing or emerging ML/TF risks associated with new games, services or procedures, including new delivery channels and technologies (**New Arrangements**).
- 117 Clause 8 in each version of the Standard Part A Programs required Crown Melbourne and Crown Perth to assess the ML/TF risk of any New Arrangement before submitting it to its respective State gaming regulator for approval, or if such approval was not required, before implementing the New Arrangement.
- 118 Clause 8 in each version of the Crown Perth Standard Program required a New Arrangement to be assessed by the relevant department using the form in Appendix H, which then had to be reviewed (and, where appropriate, approved) by the AML/CTF Compliance Officer.
- 119 Annexure J in each version of the Crown Melbourne Standard Program required Crown Melbourne to assess the New Arrangement at a meeting attended by, among others, the AML/CTF Compliance Officer, Cash Transactions Reporting Manager, General Manager Compliance, General Manager Cage, Legal Counsel, and any other relevant personnel. From 23 November 2018, these risk assessments were permitted to be undertaken by way of an approval form, in the form of Attachment 1 to Annexure J of version 8 of the Part A Program.
- 120 There was no written methodology for completing the forms directed to ML/TF risks. The forms themselves contained only limited guidance on how to assess the ML/TF risk posed by the New Arrangement. There were no procedures to ensure that any identification of ML/TF risks related to New Arrangements would be reflected in Part A controls to mitigate and manage ML/TF risks. Accordingly, the Standard Part A Programs did not enable Crown Melbourne and Crown Perth

to identify, mitigate and manage the ML/TF risks arising from New Arrangements, as required by paragraph 8.1.5(5) of the AML/CTF Rules.

- 121 In practice, New Arrangements were not always assessed. For example, the risks associated with the Suncity junket (described at paragraphs 214 and 215) were not subjected to the ML/TF risk assessment process outlined above.
- 122 The Standard Part A Programs did not include risk-based procedures for Crown Melbourne and Crown Perth to identify and assess, and report to senior management, ML/TF trends arising from, or disclosed by, the usage of designated services or channels, transaction monitoring, suspicious matter reporting, internal financial crime reporting, information from AUSTRAC and law enforcement, or the external ML/TF risk environment.

F.2 Board and senior management oversight

F.2.1 Board approval of the Standard Part A Programs

Crown Melbourne

- 123 Between 1 March 2016 and 1 November 2020, the Crown Melbourne Standard Program provided that either the Crown Melbourne Chief Executive Officer (**CEO**) or Australian Resorts CEO must approve any amendment to the Crown Melbourne Standard Program.
- 124 Between 1 March 2016 and December 2020, the Australian Resorts CEO was a single role occupied by the same person that combined the roles of both CEO for Crown Melbourne and CEO for Crown Perth.
- 125 At no time did the Crown Melbourne Standard Program require both the board of directors of Crown Melbourne (**Crown Melbourne Board**) and Crown Melbourne senior management to approve the Crown Melbourne Standard Program.
- 126 Between 1 March 2016 and 1 November 2020, each version of the Crown Melbourne Standard Program was approved by the Australian Resorts CEO, in accordance with the Crown Melbourne Standard Program. In addition, version 7 of the Crown Melbourne Standard Program was approved by the Crown Melbourne Board, and version 7.1 was approved by the Crown Melbourne Board Compliance Committee (**Compliance Committee**).
- 127 Version 8 of the Crown Melbourne Standard Program (effective from 27 November 2018 to 1 November 2020) was not approved by the Crown Melbourne Board.
- 128 As a result of the matters set out at paragraphs 123 to 127 above, between 27 November 2018 and 1 November 2020, the Crown Melbourne Standard Program did not fully comply with the requirements of paragraph 8.4.1 of the AML/CTF Rules and section 84(2)(c) of the AML/CTF Act.

Crown Perth

- 129 Between 1 March 2016 and 1 November 2020, the Crown Perth Standard Program provided that the Crown Perth CEO and / or the board of directors of Crown Perth (**Crown Perth Board**) must approve any substantive amendment to the Crown Perth Standard Program.
- 130 At no time did the Crown Perth Standard Program require both the Crown Perth Board and Crown Perth senior management to approve the Crown Perth Standard Program.
- 131 Between 1 March 2016 and 1 November 2020, the Australian Resorts CEO / Crown Perth CEO approved the following versions of the Crown Perth Standard Program:

- (a) Version 14, approved on 28 April 2015;
 - (b) Version 15, approved on 14 December 2016;
 - (c) Version 16, approved on 24 April 2017; and
 - (d) Version 17, approved on 3 December 2018.
- 132 The Crown Perth Board did not approve any version of the Crown Perth Standard Program between 1 March 2016 and 1 November 2020.
- 133 As a result of the matters set out at paragraphs 129 to 132 above, between 1 March 2016 and 1 November 2020, the Crown Perth Standard Programs did not fully comply with the requirements of paragraph 8.4.1 of the AML/CTF Rules and section 84(2)(c) of the AML/CTF Act.

F.2.2 Board and senior management oversight of the Crown Part A Programs

- 134 The AML/CTF Act and AML/CTF Rules require ongoing oversight of Part A of an entity's AML/CTF Program by the board and senior management.
- 135 A reporting entity of the nature, size and complexity of Crown Melbourne and Crown Perth, having regard to the ML/TF risks each reasonably faces, cannot adopt and maintain a Part A Program that has the primary purpose of identifying, mitigating and managing ML/TF risks reasonably faced with respect to the provision of designated services if the Part A Program does not include or establish a framework that is designed to:
- (a) determine and set the reporting entity's ML/TF risk appetite;
 - (b) set controls to ensure designated services are provided to customers consistently with that ML/TF risk appetite;
 - (c) appropriately monitor management's performance against an appropriate ML/TF risk management framework, including the reporting entity's risk appetite;
 - (d) ensure the board receives and reviews management reports about new and emerging sources of ML/TF risk and about the measures management are taking to deal with those risks; and
 - (e) establish appropriate ML/TF risk management capability frameworks, including with respect to roles and accountabilities, operational procedures, reporting lines, escalation procedures, assurance and review, and information management.
- 136 The Standard Part A Programs did not meet the requirements identified at paragraphs 134 and 135 contrary to ss 81, 84(2)(a) and 84(2)(c) of the AML/CTF Act and paragraphs 8.1.3 and 8.1.5(4) of the AML/CTF Rules.
- 137 Crown acknowledges that its boards and senior management are responsible for oversight of the management of ML/TF risks faced by its business in accordance with the AML/CTF Act and AML/CTF Rules.
- 138 Crown acknowledges that in respect of the Standard Part A Programs:
- (a) reporting to the Crown Melbourne and Crown Perth boards and senior management on AML/CTF compliance and the identification, mitigation and management of ML/TF risk reasonably faced by Crown was ad hoc and incomplete;
 - (b) neither the Crown Melbourne Board nor the Crown Perth Board determined ML/TF risk appetite for the purposes of the Standard Part A Programs;

- (c) neither the Crown Melbourne Board nor the Crown Perth Board had a documented process in place to ensure in-depth discussion of ML/TF risk as against measurable criteria at regular intervals as part of a rolling agenda;
- (d) neither Crown Melbourne nor Crown Perth completed an independent review that satisfied all of the requirements of Part 8.6.5 of the AML/CTF Rules which are for the purposes of assessing the Part A Program's compliance and effectiveness; and
- (e) there was a lack of clarity and understanding within Crown as to:
 - (i) reporting lines to and from senior management; and
 - (ii) the roles and accountabilities,
 with respect to ML/TF risk management and compliance.

139 Since November 2020, Crown's Board and senior management oversaw a range of measures directed at improving Crown's AML/CTF function and the identification, mitigation and management of ML/TF risks, including the measures outlined at section H.7 below. These improvements were directed at addressing, among other things, the shortcomings listed at paragraphs 135, 136 and 138 above.

F.3 Remittance services, Credit Facilities and CCFs

F.3.1 Credit Facilities and CCFs

- 140 A customer who had been approved for a Credit Facility or CCF (being facilities of the type described in paragraphs 52 and 46 respectively) could draw on the facility as outlined at paragraphs 53 and 47-48 respectively. The manner in which these facilities could be repaid or redeemed are outlined at paragraphs 54 and 49-50.
- 141 Credit Facilities and CCFs involved the provision by Crown Melbourne and Crown Perth of items 6 and 7, table 1 and item 13, table 3 designated services to customers.
- 142 The provision of Credit Facilities and CCFs at both Crown Melbourne and Crown Perth involved inherently higher ML/TF risks on the basis that:
- (a) Credit Facilities and CCFs could be drawn down and repaid as part of a complex chain of different designated services;
 - (b) Credit Facilities and CCFs may have enabled funds held by customers in foreign jurisdictions to be used in Australia without the need for cross-border transfers;
 - (c) Credit Facilities and CCFs could be drawn down by way of DAB deposits and withdrawn in cash (although there were limits on the extent to which a customer could draw down funds in cash and apply those funds for a non-gaming purpose);
 - (d) repayments of Credit Facilities and CCFs could be made by way of telegraphic transfer, which was a non-face-to-face channel;
 - (e) Credit Facilities and CCFs could be repaid by third parties through non-face-to-face channels until November 2020;
 - (f) junket operators and representatives were provided with significant lines of credit through Credit Facilities and CCFs; and
 - (g) Credit Facilities could be shared across Crown Melbourne and Crown Perth.

- 143 These ML/TF risks were not appropriately identified and assessed until the Enterprise Wide Risk Assessment was completed in December 2021.
- 144 As detailed at paragraph 198, the Standard Part A Programs did not include appropriate risk-based systems and controls that were capable of identifying, mitigating and managing the ML/TF risks associated with Credit Facilities and CCFs.¹³
- 145 By no later than June 2018, the Chief Legal Officer of Crown Resorts, who was also the AMLCO for both Crown Melbourne and Crown Perth, was briefed on a recommendation from the Group General Manager AML (Melbourne) that Crown's credit policies and the means of repayment from offshore be taken to the Board for its consideration as to its comfort level. The Group General Manager AML also recommended that a compliance review be conducted on all credit arrangements. This compliance review did not occur and did not prompt any review of anti-money laundering and counter-terrorism financing requirements with respect to Credit Facilities or CCFs.

F.3.2 Overseas deposit services

- 146 The overseas deposit services provided by Crown were largely governed by practice and convention rather than documented processes or procedures.

City of Dreams

- 147 Crown Melbourne and Crown Perth provided overseas deposit services to customers through the City of Dreams (**COD**) casino in Macau from approximately 2009 until October 2016, and in Manila from December 2014 until May 2017.
- 148 A mutual customer of any Crown casino and one of the COD properties could deposit funds at a COD cage in various forms, including by way of cash, chips (from COD Macau and COD Manila, or other casinos) and foreign currency (noting paragraph 151).
- 149 Crown Melbourne and Crown Perth relied on COD Macau and COD Manila to conduct identification checks on the person depositing the funds. No source of funds checks were applied by Crown Melbourne or Crown Perth on deposits via the COD deposit services. Crown does not know whether COD Macau or COD Manila undertook any source of funds checks on depositors at the cage.
- 150 The COD deposit services could be used for the following purposes:
- (a) release of funds by Crown Melbourne or Crown Perth to a customer for use as front money at Crown Melbourne or Crown Perth, as described in paragraphs 152 to 156 below; or
 - (b) to repay an amount owed by a customer to Crown Melbourne or Crown Perth under a Credit Facility or CCF, as described in paragraphs 157 to 158 below.
- 151 There was no requirement or process in place to ensure that the person depositing funds through the COD deposit service was the same person as the Crown customer accessing the funds for one of the purposes identified at paragraph 150.

¹³ See paragraphs 15 to 17 for an explanation of appropriate risk-based procedures, systems and controls.

Use of COD deposit services for front money

- 152 On receipt of a deposit, the COD cage would complete a Funds Collection Receipt, which contained the depositor's details, amount deposited and the customer to whom the funds should be made available, and email it to the Crown Melbourne or Crown Perth Cage.
- 153 Funds were not made available by Crown Melbourne or Crown Perth to the customer until the Funds Collection Receipt was received, the customer presented at the Crown Melbourne or Crown Perth Cage with identification that matched the Funds Collection Receipt and signed the relevant telegraphic transfer paperwork, and approval was obtained for the 'early release'¹⁴ of the funds to the customer (generally by at least two authorised signatories). For the early release of funds exceeding \$1 million, at Crown Melbourne one of the signatories was required to have been a member of executive management and at Crown Perth, the required signatories were two Company Officers Level 1.
- 154 Approved funds were made available by Crown Melbourne or Crown Perth to the customer by crediting the money to the customer's DAB. After approved funds were credited to a customer's Crown Melbourne or Crown Perth DAB, the customer could:
- (a) draw those funds out as a CPV to obtain program chips; or
 - (b) in certain circumstances, transfer some of those funds to another customer's DAB to enable that customer to use those funds as front money for a program; or
 - (c) for some program players at Crown Melbourne only, cash out up to five percent of the approved funds, or up to a set cash out limit approved by Crown's VIP International senior management. The cash out was intended to be applied for a non-gaming purpose, such as towards shopping or holiday expenses during the customer's trip.
- 155 At the conclusion of a program the Crown Melbourne or Crown Perth Cage would notify the COD cage of the amount won or lost by the customer as compared with the amount that had been released to them as front money and credited to their DAB, and:
- (a) if the customer had won more than the amount that had been credited to the customer's DAB, then the COD cage would make the original deposit available for collection to the original depositor at the COD cage, and the Crown Melbourne or Crown Perth Cage paid the customer any amount that was won over and above the amount that had been credited to the customer's DAB; or
 - (b) if the customer had lost some or all of the amount that had been credited to the customer's DAB, then:
 - (i) the customer was required to apply any proceeds of the customer's program to the repayment of the front money;
 - (ii) to the extent of the shortfall (ie, the amount lost by the customer), the COD cage would transfer the equivalent amount from the original deposit from its bank account to Crown Melbourne or Crown Perth's bank account; and
 - (iii) as an alternative to (ii), the customer could pay the amount of the loss to Crown Melbourne or Crown Perth by way of telegraphic transfer or bank draft. If this occurred, Crown Melbourne or Crown Perth would notify the COD cage that the

¹⁴ Early release means that funds were made available to a Crown customer at a point in time before any funds were received by Crown.

customer had paid the amount of the loss and the COD cage would make the original deposit available for collection at the COD cage to the original depositor.

- 156 Where some or all of the original deposit was to be returned to the original depositor, it could not be collected by anyone other than the original depositor and had to be collected in the same form as it was deposited (eg, cash or chips).

Use of COD deposit services for repayment of Credit Facility or CCF

- 157 A customer could arrange for a debt owed to Crown Melbourne or Crown Perth under a credit facility or CCF to be repaid through the COD deposit service.
- 158 The depositor was required to notify COD that the deposit was being made to repay a debt owed to Crown Melbourne or Crown Perth by a customer. Following verification of the debt owed by the customer and proof of the customer's loss, the funds would then be transferred from a COD bank account to one of Crown Melbourne's or Crown Perth's bank accounts in full or partial satisfaction of the debt owed by the customer to Crown Melbourne or Crown Perth.

Crown Aspinalls London

- 159 During the Relevant Period until August 2019, Crown Melbourne and Crown Perth provided overseas deposit services to customers through Crown Aspinalls London (**Crown Aspinalls**), a members-only casino owned by the Crown Resorts group.
- 160 The Crown Aspinalls deposit service operated in a similar manner to the COD deposit services, as described in paragraphs 147 to 158 above. Money was made available by Crown Melbourne or Crown Perth through this service to the customer by crediting the money to the customer's DAB.

The South East Asian deposit service offered by Company 10

- 161 During the Relevant Period until September 2020, Crown provided overseas deposit services to customers through a company based in South East Asia (**Company 10**).
- 162 Company 10 was a money changer operated by Person 56. Person 56 was also the majority shareholder in Company 10. Person 56 was a customer of Crown Melbourne and Crown Perth, as well as a junket tour representative and key player with a junket at Crown Melbourne.
- 163 A person could deposit funds with Company 10 for play on a junket or premium player program at Crown Melbourne or Crown Perth. Crown Melbourne and Crown Perth did not conduct identification, source of funds or wealth checks on the person who deposited the funds with Company 10.
- 164 Person 56 provided Crown Melbourne and Crown Perth with a letter confirming the amount that was held on behalf of a customer. In reliance upon this letter, Crown Melbourne or Crown Perth approved the early release of funds to its customer. Approved funds were made available by Crown Melbourne or Crown Perth through this service to the customer by crediting the money to the customer's DAB.
- 165 The original deposit was held by Company 10 until the customer's play on the program had concluded. The process at the conclusion of a program was similar to that described in paragraph 155 above for the COD deposit services.

ML/TF risks of overseas deposit services

- 166 The overseas deposit services referred to above involved the provision by Crown Melbourne and Crown Perth of item 32, table 1, section 6, designated services to customers. The overseas deposit services were designated remittance arrangements. Crown provided these services in the course of carrying on a business giving effect to remittance arrangements. Through these designated remittance arrangements, Crown made money available to customers.
- 167 At no time did Crown Melbourne or Crown Perth carry out an ML/TF risk assessment of the designated services provided through overseas deposit services.
- 168 The provision of overseas deposit services at both Crown Melbourne and Crown Perth involved inherently higher ML/TF risks on the basis that:
- (a) overseas deposit services were used as part of a complex chain of different designated services;
 - (b) overseas deposit services may have enabled funds held by customers in foreign jurisdictions to be used in Australia without the need for cross-border transfers (although such funds were generally intended by Crown to be applied to gaming by the customer) For example, between 1 November 2018 and 14 November 2018, Crown Perth agreed to make \$500,000 in front money available to a junket operator, Person 8, by offsetting funds deposited offshore by Person 8 with Company 10 without an accompanying cross-border transfer. Person 8 was known by Crown Perth to be playing alongside Customer 5, but Crown Perth was unable to confirm whether any chips were exchanged between them. IFTIs were reported to AUSTRAC in respect of the offset transaction;
 - (c) overseas deposit services could be released by way of DAB deposits and, at Crown Melbourne, withdrawn in cash (although there were limits on the extent to which a customer could withdraw funds in cash and apply those funds for a non-gaming purpose);
 - (d) losses associated with overseas deposit services could be paid by telegraphic transfer, which was a non-face-to-face channel;
 - (e) losses associated with overseas deposit services could be paid by third parties through non-face-to-face channels up until November 2020;
 - (f) third party transactions could be facilitated through overseas deposit services involving ML/TF risks as to the source of funds;
 - (g) Crown Melbourne and Crown Perth customers accessing funds via an overseas deposit service did not need to be the same person as the depositor up until November 2020;
 - (h) some aspects of overseas deposit services lacked transparency; and
 - (i) overseas deposit services were an avenue for potential money laundering through smurfing or cuckoo smurfing.
- 169 The Standard Part A Programs did not include appropriate risk-based systems and controls that were capable of identifying, mitigating and managing the ML/TF risks associated with overseas deposit services.¹⁵ In particular:
- (a) The approval of the release of funds for use as front money did not have regard to ML/TF risk assessments.

¹⁵ See paragraphs 15 to 17 for an explanation of appropriate procedures, systems and controls.

- (b) The Standard Part A Programs did not include any controls requiring the customer accessing funds via an overseas deposit service to be the same person as the depositor, or controls for Crown Melbourne or Crown Perth to verify that the depositor and customer were the same person.
- (c) The Standard Part A Programs did not include any controls to prevent third parties remitting money to Crown customers prior to November 2020.

F.3.3 Bank account and DAB transactions

170 Subject to paragraph 173 below, a customer could instruct Crown Melbourne or Crown Perth to transfer money via telegraphic transfer from their DAB or SKA to:

- (a) a bank account for the purposes of returning front money or remitting winnings; or
- (b) until 21 May 2021, another casino, including an Australian or foreign casino.

171 Subject to paragraph 173 below, a customer could deposit money, or arrange for money to be deposited, into a Crown Patron Account to:

- (a) transfer front money for a visit to the casino;
- (b) repay an amount owed to Crown; or
- (c) until 21 May 2021, transfer funds from another casino, including an Australian or foreign casino.

Crown would then make the deposited money available to the customer by crediting the money to the customer's DAB.

172 The transactions described at paragraphs 170 to 171 above involved the provision by Crown Melbourne and Crown Perth of items 31 and 32, table 1 designated services to customers. These services involved the transfer of money under a designated remittance arrangement. Crown provided these services in the course of carrying on a business giving effect to remittance arrangements. Through these designated remittance arrangements, Crown accepted instructions for the transfer of money from customers, and made money available to customers. These designated services were provided through the Crown Patron Account channel.

173 Prior to November 2020, Crown permitted third parties to deposit money into a customer's DAB or SKA via the Crown Patron Account channel. Prior to November 2020, Crown also facilitated the transfer of funds from a customer's DAB or SKA to a third party, via telegraphic transfers through the Crown Patron Account channel:

- (a) On 8 April 2020, Crown Melbourne and Crown Perth circulated a memorandum stating that it would no longer make or receive payments to or from third parties without prior written approval from the relevant Chief Operating Officer (COO) and Group General Manager AML.
- (b) However, this policy was not formalised until October 2020.
- (c) It was not until 16 November 2020 that manual weekly reviews of bank statements commenced to identify deposits from third parties to enable the policy to be enforced.
- (d) It was not until January 2021 that Crown formalised a policy to return money received in breach of the Third Party Transfers and Money Remitters Policy.

- 174 Prior to November 2020, Crown permitted customers to transfer money from their DAB to another customer's DAB. This involved the provision by Crown Melbourne and Crown Perth of items 31 and 32, table 1 designated services to customers. These services involved the transfer of money under a designated remittance arrangement. Crown provided these services in the course of carrying on a business giving effect to remittance arrangements. Through these designated remittance arrangements, Crown accepted instructions for the transfer of money from customers, and made money available to customers.
- 175 Items 31 and 32, table 1, section 6 of the AML/CTF Act designated services involved higher ML/TF risks, including:
- (a) Money could be remitted 24 hours a day 7 days a week, including offshore.
 - (b) Remittance services were often provided as part of a complex chain of different designated services under tables 1 and 3, section 6 of the AML/CTF Act.
 - (c) Many remittance services were not provided face-to-face.
- 176 The ML/TF risks associated with items 31 and 32, table 1, section 6 of the AML/CTF Act designated services (and the Crown Patron Account channel), and the associated risk-based systems and controls in place, are further addressed in section E.4.2 below. At no time did Crown conduct an appropriate assessment of the ML/TF risks of providing items 31 and 32, table 1 and table 3, section 6 of the AML/CTF Act designated services through DABs or through the Crown Patron Account channel.
- 177 By no later than June 2018, the Chief Legal Officer of Crown Resorts, who was also the AMLCO for both Crown Melbourne and Crown Perth, was advised by the Group General Manager AML (Crown Melbourne) that third party deposits were being accepted into DABs with very limited checks as to the identity of the third party or their source of funds. The Chief Legal Officer/AMLCO was advised there was a potential vulnerability that these third party deposits were from an illicit source. The briefing recommended that Crown Melbourne's willingness to accept third party transfers and/or deposits without conducting further KYC or other due diligence to understand the source of funds be taken to the Crown Melbourne Board for consideration, as it raised questions of risk appetite.

F.3.4 Suncity account

- 178 In May 2017, a Crown Resorts employee opened an account in their personal name with Suncity in Macau (the **Suncity account**). The Suncity account was intended to be used to receive debt repayments to Crown Melbourne, Crown Perth and Crown Aspinalls.
- 179 Shortly after the Suncity account was put in place, Crown revisited its decision to offer this service due to concerns around Suncity's application of its local AML obligations identified by the Chief Legal Officer of Crown Resorts and AMLCO for both Crown Melbourne and Crown Perth.
- 180 Funds were held in the Suncity account in circumstances where the customer's source of funds was unknown. In June 2017, Crown Melbourne agreed to a proposed transaction through the Suncity account in settlement of an AUD\$9.6 million debt owed to Crown Melbourne by a former customer (Customer 27). Crown Melbourne agreed that the debt amount would be settled by payment of 50 per cent of the debt amount. Customer 27 arranged for a deposit in HKD of an equivalent of AUD\$4.8 million into the Suncity account. However, this amount was never remitted via the Suncity account to Crown Melbourne. In April 2018, Crown Melbourne agreed to offset the equivalent of AUD\$4.8 million in HKD deposited on behalf of Customer 27 into the

Suncity account against 'lucky money' that Crown Melbourne itself owed to the Suncity junket operator, Customer 1.

181 The transaction described in paragraph 180 above involved the provision by Crown Melbourne of an item 32, table 1 designated service whereby money was made available to a customer as a result of a transfer under a designated remittance arrangement, in the course of carrying on a business of giving effect to remittance arrangements. Crown did not conduct any formal ML/TF risk assessment in relation to the Suncity account.

182 As at January 2018, the Suncity account held approximately AUD\$22.3 million. In March 2018, funds remaining in the Suncity account were to be returned to the original depositors, after which time the services of Company 10 (see paragraphs 161 to 165) were used to remit some of the funds from the original depositors to either Crown Melbourne or Crown Perth. The ML/TF risks of the overseas deposit service of Company 10 were not assessed.

F.3.5 The Hotel Card channel

183 During the Relevant Period until October 2016, Crown Melbourne made money available to customers through the Hotel Card channel as described in paragraph 56 above. This involved the provision of item 32, table 1, section 6 designated services. Crown Melbourne made money available to the customer through the Hotel Card channel, as a result of a transfer under a designated remittance arrangement, by entering a credit onto the customer's DAB or by providing the customer with a CEV. Crown provided these services in the course of carrying on a business giving effect to remittance arrangements. At no time did Crown conduct an ML/TF risk assessment of providing table 1 and table 3, section 6 designated services through the Hotel Card channel.

F.4 Risk-based systems and controls

184 To comply with the provisions in the AML/CTF Rules described in Section D, a Standard Part A Program and a Joint Part A Program must include appropriate risk-based systems and controls which are aligned and proportionate to the reporting entity's current ML/TF risks as identified in risk assessments, having regard to the matters described in paragraph 8.1.3 (for Standard programs) or paragraph 9.1.3 (for Joint Programs) of the AML/CTF Rules. Further, a Part A Program will not be capable of having the primary purpose specified in section 84(2)(a) (for Standard Programs) or section 85(2)(a) (for Joint Programs), if it does not include appropriate risk-based systems and controls that are capable by design of identifying, mitigating and managing ML/TF risks reasonably faced by the reporting entity, consistent with the risk appetite determined by Board and senior management.¹⁶

185 As described in E.1 and E.2 above, from 1 March 2016 to 1 November 2020, Crown Melbourne and Crown Perth did not appropriately assess the inherent and residual ML/TF risks associated with their provision of designated services. As a result, and as described in paragraphs 187 to 201 below, the systems and controls in the Standard Part A Programs were not able to appropriately address the ML/TF risks that Crown Melbourne and Crown Perth reasonably faced across all designated services. Nor did the Board and senior management determine ML/TF risk appetite; nor did they determine what risk-based controls were required to manage ML/TF risks within an appropriate ML/TF risk appetite.

¹⁶ See paragraphs 15 to 17 for an explanation of appropriate procedures, systems and controls.

186 As a consequence, between 1 March 2016 and 1 November 2020, the risk-based systems and controls in the Standard Part A Programs did not fully comply with the requirements of paragraph 8.1.3 of the AML/CTF Rules and sections 84(2)(a) and 84(2)(c) of the AML/CTF Act.

F.4.1 Designated services

187 Save as where indicated otherwise below, from 1 March 2016 to 1 March 2022, Crown Melbourne and Crown Perth provided the designated services listed in paragraph 10 through:

- (a) **DABs and SKAs.** DABs and SKAs were used by customers for transactions involving the provision of items 31 and 32, table 1 and items 7, 8, 11 and 13, table 3 designated services (see description in paragraphs 34 – 38);
- (b) **Crown Patron Accounts,** as referred to in paragraphs 28 to 33, 35. The term Crown Patron Accounts refers to bank accounts held by Crown Melbourne and Crown Perth, respectively, in both AUD and foreign currency. Funds deposited or withdrawn into or out of Crown Patron Accounts would be credited or debited to a customer's DAB or SKA. The Crown Patron Accounts were channels through which items 31 and 32, table 1 and item 13, table 3 designated services were provided to customers;
- (c) **The overseas deposit services** as referred to in Section F.3.2, involving the provision of item 32, table 1, section 6 designated services. These services ceased on the dates set out in paragraph 57;
- (d) **Credit Facilities and CCFs,** as referred to at paragraphs 46 to 55 and 140 to 145, involving the provision of items 6 and 7, table 1, section 6 designated services. Funds Advance Facilities and CCFs ceased to be offered at Crown Perth from 23 February 2021 and 31 December 2021 respectively; Credit Facilities at Crown Melbourne ceased to be offered from 30 June 2021;
- (e) **Card Play, Card Play Extra and Cashless accounts,** which allowed customers playing on gaming machines to transfer funds from their DABs to their cards, or credits between their Crown Rewards cards and gaming machines (see description in paragraphs 41 – 45). Those accounts involved the provision of items 6, 9, and 13, table 3 designated services to customers;
- (f) **Hotel Card channel,** which allowed customers to transfer funds from their debit or credit cards at the Crown Towers Hotel for use at the Crown Melbourne casino (see description in paragraph 56). The Hotel Card channel involved the provision of items 7 and 13, table 3, and item 32, table 1, section 6 of the AML/CTF Act designated services to customers. This service ceased in October 2016;
- (g) **exchanging money for CVIs, including chips and tokens** (see description in paragraph 26). This process involved the provision of items 6, 7, 8, 9, 13, table 3 designated services to customers;
- (h) **table games and EGMs** (see description in paragraph 24). Table games and EGMs involved the provision of items 6 and 9, table 3 designated services to customers; and
- (i) **foreign currency exchange services** (see description in paragraph 59) which involved the provision of item 14, table 1 designated services to customers.

188 The designated services listed in paragraph 187 above could involve one or more of the following:

- (a) foreign currencies (see description at paragraph 59);

- (b) cash; and
- (c) third party transactions (see description at Schedule 2).

F.4.2 ML/TF risks of the designated services

189 The designated services referred to in section F.4.1 above involved ML/TF risks, including the following:

(a) DABs and SKAs:

- (i) DABs and SKAs could be used to facilitate the movement of money into and out of the casino environment through complex transaction chains, presenting opportunities for layering of laundered funds.
- (ii) Until November 2020, third parties could deposit funds into DABs and SKAs via cash or telegraphic transfer, and receive funds from DABs and SKAs. Funds could also be transferred between DABs and SKAs of different customers (although after November 2020 this was on an exception basis only). These attributes created risks relating to the source of funds and exposed Crown Melbourne and Crown Perth to ML/TF typologies such as cuckoo smurfing.
- (iii) A customer could withdraw funds from their DAB or SKA via TT or cheque, including when the customer had applied the funds to minimal or no gaming. This presented opportunities to integrate laundered funds into the financial system. A customer could also withdraw funds from their DAB or SKA by way of cash, including when the customer had applied the funds to minimal or no gaming.
- (iv) Customers and third parties could withdraw funds from DABs and SKAs without being face-to-face by completing Authority to Disperse Forms (completed when a customer was not on site), creating opportunities for layering of funds. From November 2020, third parties were prohibited from engaging in this conduct (with limited exceptions, such as when payments were made from a junket operator's deposit account with Crown to a key player provided that the proposed transfer of funds was consistent with the key player's gaming activity recorded under the relevant junket program, noting the limitations at paragraphs 205(b) and (c)(iii), 211 and 212(b); or if prior written approval was obtained from the COO of the relevant Crown entity and the Group General Manager – AML).
- (v) Crown Melbourne and Crown Perth provided customers with multiple DABs, sometimes with different customer (or patron) identification numbers (known as **PIDs**) and sometimes in pseudonyms. Funds could be transferred between these accounts.
- (vi) DABs and SKAs could also be used to 'park' funds, putting distance between an act or acts that generated illicit funds and the ultimate recipients of those funds, making it more difficult to understand or trace the flow of money. DABs or SKAs held by junket operators or representatives were highly vulnerable to the storage and movement of potentially illicit funds. By no later than June 2018, the Chief Legal Officer of Crown Resorts, who was also the AMLCO for both Crown Melbourne and Crown Perth, was advised that the AML Team in Melbourne infrequently checked for parked monies.

- (b) **Crown Patron Accounts:**
- (i) Designated services provided through the Crown Patron Accounts involved DABs and SKAs and accordingly also involved the ML/TF risks set out in paragraph 187(a) above.
 - (ii) Funds, including cash, could be deposited into Crown Patron Accounts through non-face-to-face channels, which created risks as to the source of funds.
 - (iii) Funds could be moved across international borders through Crown Patron Accounts.
 - (iv) Junket operators, money remitters, overseas deposit services and individuals used these accounts until November 2020, which created risks as to the source of funds. Acceptance of third-party payments into Crown Patron Accounts may have provided an avenue for money laundering through smurfing or cuckoo smurfing.
 - (v) The Southbank and Riverbank Crown Patron Accounts involved the following additional ML/TF risks:
 - (A) Crown's association with those accounts was not immediately apparent as the accounts operated in the names of Southbank Investments Pty Ltd, a wholly owned subsidiary of Crown Melbourne, and Riverbank Investments Pty Ltd, a wholly owned subsidiary of Burswood Ltd.
 - (B) Some customer deposits were entered with the description 'investment', which may have disguised the purposes of the deposits.
 - (C) On several occasions from January 2014, banks put Crown Melbourne and Crown Perth on notice that money laundering may have been occurring through the Southbank and Riverbank accounts.
 - (D) An external auditor's report concluded that the value of deposits into the Southbank and Riverbank accounts between 2013 and 2019, with features indicative of money laundering, was over \$290 million.
- (c) **Overseas deposit services:** These designated services involved the ML/TF risks set out in paragraph 168 above, including risks associated with complex transaction chains and a lack of transparency as to source of funds.
- (d) **Credit Facilities and CCFs:** These designated services involved the ML/TF risks set out in paragraph 142 above. The provision of Credit Facilities and CCFs to junket operators involved heightened ML/TF risks because Crown had no visibility as to how the operator funded junket players' front money, how gaming chips obtained through approved junket credit were distributed amongst junket players, how winnings were distributed to junket players and as to the source of funds for the repayment or redemption of credit and CCFs. In mid-2018, it was recommended to the Crown AMLCO that Crown's credit policies and the means of repayment from offshore be taken to the Board for its consideration as to its comfort level and that a compliance review be conducted on all credit arrangements. This compliance review did not occur and did not prompt any review of AML/CTF requirements with respect to Credit Facilities or CCFs.
- (e) **Hotel Card channel:** The channel lacked transparency, including because money obtained through the channel could be deposited into a customer's DAB and could be

withdrawn in cash, or transferred to third parties, or money could be redeemed by a CEV or CPV. Additionally, the jurisdictional risk profile of the customers using the Hotel Card channel was generally high and there was a heightened risk that the channel facilitated the transfer of capital out of jurisdictions in breach of capital control laws. A significant proportion of withdrawal activity connected to Hotel Card channel deposits was remitted to junket operators.

- (f) **Exchanging money for CVIs, including chips and tokens:** Chips could be purchased with cash generated through criminal activity, then redeemed by casino cheque or money transfer to integrate funds into the formal financial system. CVIs were highly transferrable, could not always be traced to an account holder or identified customer, and could be issued in large values. CVIs could be used to layer funds, as part of a more complex transaction chain of designated services, making it difficult to understand the purpose of transactions, the beneficial owner of funds or the ultimate beneficiary of value moved. The redemption of CVIs could not always be attributable to winnings and could be cashed out with minimal or no play. The issue or redemption of tickets was not always face-to-face.
- (g) **Table games and EGMs:** In table games that permitted even money wagering, such as roulette and baccarat, two customers could cover both sides of an even bet to give the appearance of legitimate gaming activity while minimising net losses. Baccarat also involved a low 'house edge' and each hand could be high in value and played within seconds. Money could therefore be turned over quickly, with minimal net loss and in collusion with other players. Poker permitted peer-to-peer gaming, which posed risks of collusion. The risks of even-money wagering were higher with certain semi-automated and fully-automated games, as there was inappropriate oversight and a player could play several terminals at the same time. Money including cash could be inserted into ETGs and EGMs, and tickets could be collected with minimal or no play. EGMs and ETGs are vulnerable to refining because they process large volumes of smaller amounts quickly. Money could also be moved through table games and EGMs through buying-in and cashing-out using cash, chips, TITO tickets and other CVIs. Play on table games and EGMs could be used to layer funds, as part of a more complex transaction chain of designated services, making it difficult to understand the purposes of transactions, the beneficial owner of funds or the ultimate beneficiary of value moved.
- (h) **Card Play Extra:** Cash could be deposited and withdrawn from Card Play Extra accounts, without appropriate risk-based limits for customers with certain Crown Rewards members tiers.¹⁷ Funds from DABs could be transferred to Card Play Extra accounts, including funds that had been deposited in DABs via the Crown Patron Account channel.
- (i) **Foreign currency exchange:** Foreign currency exchange posed the following ML/TF risks: bank drafts/cheques cashed in for foreign currency, multiple currency exchanges, dramatic or rapid increases in size and frequency of currency exchange transactions for regular account holders, currency exchange for no reasonable purpose, currency exchanges with low denomination bills for high denomination bills, currency exchanges carried out by third parties, large, one-off, or frequent currency exchanges for customers not known to the casino, requests for casino cheques from foreign currency, and currency exchanges with little or no gambling activity.

¹⁷ See paragraph 13 on the risks of cash.

190 The ML/TF vulnerabilities, techniques and typologies involving cash, foreign currency and third party transactions are set out in **Schedule 2**.

F.4.3 Risk Assessments

191 Section F.1 addresses the way in which each of Crown Melbourne and Crown Perth identified and assessed its ML/TF risks in relation to a number of designated services provided by each entity.

192 Through this approach, neither Crown Melbourne nor Crown Perth identified all the ML/TF risks referred to in paragraph 189 above. The ML/TF risks the Risk Registers did identify are described in section F.1.

F.4.4 Risk-based systems and controls

193 ML/TF risk-based systems and controls may be either 'preventative' or 'detective':

- (a) Preventative controls are those that limit the ability to use a product or channel in a way that would increase ML/TF risk. Examples of preventative controls include: setting transaction limits, having a management approval process for high-risk customers, products or countries, applying different identification processes for customers not dealt with in person, and not accepting customers who are deemed too high risk.
- (b) Detective controls only seek to monitor activity through a product or channel. Examples of detective controls include: gathering information about how products or channels are used and reviewing information from internal records, such as transaction monitoring and suspicious matter reporting. Detective controls do not, of themselves, reduce inherent ML/TF risks.

194 The AML/CTF Act and AML/CTF Rules require a reporting entity to have regard to a number of factors in determining the appropriate risk-based procedures, systems and controls that it will include in Part A of its AML/CTF Program. These factors are detailed at paragraphs 15 to 17 above.

195 The Standard Part A Programs included some risk-based systems and controls intended to address the ML/TF risks of providing the designated services referred to in section F.4.1. However:

- (a) the controls in the Standard Part A Program were not appropriately aligned and proportionate to the ML/TF risks reasonably faced by Crown Melbourne and Crown Perth with respect to the provision of designated services, as set out at paragraph 189; and
- (b) the controls that were included in the Standard Part A Program were focused more on detection of ML/TF risks, rather than prevention, and did not appropriately mitigate and manage the ML/TF risks reasonably faced by Crown Melbourne and Crown Perth.

196 The Standard Part A Programs did not include appropriate risk-based preventative controls with respect to **cash**. For example:

- (a) There was no mandatory requirement to obtain information or verification of source of funds for large cash deposits at the Cage or into Crown Patron Accounts.
- (b) Prior to December 2020, approval levels for large cash transactions at the Cage were inadequate.
- (c) It was not until November 2020 that cash deposits over \$250,000 (in aggregate across a calendar day or in a single transaction) were no longer permitted at the Cage, noting that

from this point in time cash deposits of over \$200,000 had to be accompanied by source of funds declaration and written approval from either the property COO, Chief Financial Officer of Crown Resorts and the Group AMLCO or Group GM Risk and Audit.

- (d) Prior to November 2020, there were no limits with respect to cash payouts at the Cage, subject to subparagraph (e).
- (e) From 23 November 2018 (at Crown Melbourne) and 3 December 2018 (at Crown Perth) until 11 November 2020, a \$300,000 cap on cash transactions in any 24-hour period was introduced for junket operators, junket representatives and key players. Apart from this cap, the Standard Part A Programs did not include any other caps or limits on large cash transactions.
- (f) There were no limits on cash withdrawals from a DAB.
- (g) Between November 2020 and January 2021 Crown contacted customers to inform them they would no longer accept cash deposits and third party transfers into the Crown Patron Accounts. This decision was due to the risks of facilitating structuring, smurfing and cuckoo smurfing. Prior to November 2020, Crown Melbourne and Crown Perth did not seek to prohibit or restrict third party payments to or from Crown Patron Accounts, exposing Crown to risks concerning source of funds and to typologies such as cuckoo smurfing. However, after November 2020, Crown was not able to consistently identify and return cash that had been deposited into its accounts, due to limitations in the transactional data received from its bankers.
- (h) Crown Melbourne and Crown Perth did not impose limits on the amount of cash that could be held in a patron's DAB or SKA, or the time period in respect of which cash could be held in a patron's DAB or SKA, exposing Crown to risks such as parking of illicit funds.
- (i) Controls on cash in private gaming rooms were inadequate, in spite of Crown Melbourne's and Crown Perth's awareness of repeated suspicious activity involving very large amounts of cash: see paragraph 218. Nor were controls relating to the carrying of cash on Crown's private jets adequate.
- (j) There were no appropriate daily or transaction limits on cash deposits and withdrawals through Card Play Extra accounts for customers with certain Crown Rewards members tiers.¹⁸

197 The Standard Part A Programs did not include appropriate risk-based preventative controls with respect to **third party transactions**. For example:

- (a) Prior to November 2020, Crown Melbourne and Crown Perth did not prohibit or restrict third party payments to or from Crown Patron Accounts, exposing Crown to risks concerning source and destination of funds and to typologies such as cuckoo smurfing.
- (b) The Standard Part A Programs did not include appropriate risk-based systems or controls to understand the source of funds of deposits into Crown Patron Accounts by junket operators, money remitters, and through overseas deposit services. Nor did it include appropriate systems or controls to identify cash deposits into Crown Patron Accounts and

¹⁸ The maximum amount a customer could deposit into, or withdraw from, a Card Play Extra account at the Cage depended on their tier level of membership with Crown Rewards. At Crown Melbourne, these limits were \$2,000 for tiers up to Silver, \$50,000 for Gold tier, \$75,000 for Platinum tier, \$250,000 for Black tier and \$500,000 for Exclusive Black tier. At Crown Perth, these limits were \$40,000 for Gold tier and \$100,000 for Platinum and Black tiers.

to understand the source of these funds. In these circumstances, Crown was unable to identify whether the customer or a third party was the beneficial owner of funds.

- (c) Monies owed by customers to Crown Melbourne or Crown Perth could be settled by a third party through remittance services and overseas deposit services, where Crown Melbourne or Crown Perth had no risk-based systems or controls to understand who the third party was or their source of funds.
- 198 The Standard Part A Programs did not include appropriate risk-based controls, including preventative controls, with respect to Credit Facilities and CCFs (items 6 and 7, table 1 designated services) identified at F.3:
- (a) The approval of credit and credit limits under Credit Facilities and CCFs was subject to credit risk assessments not ML/TF risk assessments.
 - (b) The Standard Part A Programs did not include appropriate preventative controls to mitigate and manage the ML/TF risks of items 6 and 7, table 1 designated services, such as controls to:
 - (i) impose limits on credit;
 - (ii) identify customers to whom the provision of credit was outside of risk appetite; and
 - (iii) restrict the ability of third parties to repay the provision of credit on behalf of customers.
 - (c) The Standard Part A Programs did not include controls to monitor drawdowns under Credit Facilities and CCFs.
 - (d) The Standard Part A Programs did not have any processes in place to identify how, for example, the gaming chips issued by Crown, based on the approved junket credit, were subsequently distributed among the junket players by the junket operator or representative.
- 199 The Standard Part A Programs did not include appropriate risk-based controls, including preventative controls, with respect to the **remittance services** identified at F.3.
- (a) In mid-November 2020, Crown issued a policy stating that it would not accept payments to, or from, third parties (including remittance service providers and money changers) into its accounts on behalf of, or for the benefit of, a Crown customer without the prior written approval from the Property COO and the AMLCO.
 - (b) Between November 2020 and January 2021 Crown contacted customers to inform them that it would no longer accept third party transfers into Crown Patron Accounts, including from remitters.
 - (c) In January 2021, Crown issued a Return of Funds Policy applying to deposits into Crown Patron Accounts contrary to the November 2020 policy.
 - (d) Crown continued to facilitate the remittance of money between DABs held in different customer names.
 - (e) The Standard Part A Programs did not include appropriate risk-based controls to mitigate and manage the ML/TF risks associated with the provision of remittance services as part of a complex chain of different designated services under tables 1 and 3, section 6 of the AML/CTF Act.

- (f) The Standard Part A Programs had no risk-based processes in place to understand the source of funds deposited and remitted through the Crown Patron Account channel.
 - (g) The Standard Part A Programs did not include appropriate risk-based controls to mitigate and manage the ML/TF risks associated with the provision of remittance services through the overseas deposit services, as detailed at paragraph 169 and through the Suncity account channel as detailed at section F.3.4.
 - (h) The Standard Part A Program did not include appropriate preventative controls such as controls to impose daily or transaction limits on remittance.
- 200 Nor did the Standard Part A Programs include appropriate risk-based controls with respect to table 3, section 6 of the AML/CTF Act **gaming services**. For example:
- (a) With respect to table games and EGMs, the Standard Part A Programs did not include appropriate preventative controls, such as appropriate transaction or daily limits, with respect to buy-ins and cash-outs, and non-transferrable TITO tickets.
 - (b) Crown did not implement a control on tickets, as suggested in June 2018 by the Group General Manager (AML). The recommendation was made to the Chief Legal Officer of Crown Resorts and AMLCO for Crown Melbourne and Crown Perth that limits on tickets be reduced to below \$10,000 and that, in the absence of this change, this limit be taken to the Board for consideration of its comfort level.
 - (c) The Standard Part A Programs did not include appropriate risk-based procedures to understand source of wealth or funds with respect to items 6 and 9, table 3, section 6 of the AML/CTF Act designated services (especially with respect to uncarded play).
 - (d) The Standard Part A Programs did not include appropriate risk-based controls to mitigate and manage the ML/TF risks associated with the provision of table 3, section 6 of the AML/CTF Act gaming services as part of a complex chain of different designated services.
- 201 Many of the detective controls in place were not appropriate, having regarding to the ML/TF risks faced. For example:
- (a) In accordance with Crown Melbourne's TMP, the AML team regularly reviewed the deposits credited to DABs or SKAs against gaming and other activity undertaken. This review was undertaken to ascertain whether the funds were used for gaming purposes and to otherwise assess the ML/TF risks posed by customers. However, this process did not have a full view of the complex chains of designated services that were provided to customers and therefore could not consistently identify these risks. Further, at Crown Melbourne this involved extracting a daily report covering all transactions for the prior day which was then reviewed for any transactional activity that might raise concerns. However, Crown's internal process of aggregating multiple individual cash deposits into the Crown Patron Accounts that had been made in favour of the same customer obscured the number and value of the deposits in the underlying bank accounts. This inhibited Crown's ability to identify potential structuring activity and to report this activity to AUSTRAC. The practice of aggregation stopped at Crown Melbourne in November 2020.
 - (b) There were no clear internal processes setting out the frequency of checks on DABs and SKAs with infrequent use, which meant that parked funds were not closely monitored by Crown, and that large balances lay dormant in accounts, sometimes for periods greater than three months.

- (c) Manual and observational controls were not capable of consistently detecting the use of table games, ETGs and EGMs to layer funds, as part of a more complex transaction chain of designated services. The Part A detective controls did not allow the Cage visibility over any unusual patterns of activity on table games and EGMs at the point in time when the Cage exchanged chips, TITO tickets or other CVIs for money.
- (d) Manual detective processes were not supported by adequate ML/TF risk awareness training for Crown staff.
- (e) Limited transaction monitoring was applied to Card Play Extra accounts and there were no controls to identify whether money was being withdrawn from these accounts with little or no play, with the exception of surveillance from security staff.

F.5 Junkets

F.5.1 ML/TF risks of designated services provided through the junket channel

- 202 As stated in paragraph 71 above, the provision of designated services through junket channels involved higher ML/TF risks.
- 203 From 1 March 2016 until August 2020, Crown provided a range of designated services to customers through junket channels which involved complex transaction chains, but did not appropriately identify, mitigate or manage the associated ML/TF risks as required by paragraph 8.1.3 of the AML/CTF Rules.
- 204 Notwithstanding the higher ML/TF risks, the controls in the Standard Part A Programs that applied to the provision of designated services through junkets were generally no different to the controls applied to other customers.¹⁹

F.5.2 Assessment of customer ML/TF risk under the Standard Programs

- 205 Despite the known high risks associated with junkets, customers receiving designated services through junket programs were considered low risk by default. Customers receiving designated services through junket channels included junket operators, junket representatives and junket players. The Standard Programs also did not:
 - (a) provide for the assessment of jurisdictional risks associated with customers receiving designated services through the junket channel;
 - (b) include appropriate risk-based controls to appropriately identify, mitigate and manage the ML/TF risks of providing designated services to junket players through junket operators and representatives as agents. Crown's records of junket play did not always reliably or comprehensively attribute gaming to key players; or
 - (c) require Crown Melbourne and Crown Perth to:
 - (i) obtain and analyse source of wealth and funds information with respect to junket operators, representatives and players; or
 - (ii) collect and verify appropriate KYC information with respect to junket operators and other customers receiving designated services through junket channels, such as the beneficial ownership of funds or the beneficiaries of transactions; or
 - (iii) appropriately understand its business relationship with customers who were junket players. Instead, Crown Melbourne and Crown Perth relied upon the junket

¹⁹ See paragraphs 15 to 17 for an explanation of appropriate risk-based procedures, systems and controls.

operator as an intermediary or agent and consequently did not always understand the nature and purpose of the business relationship with junket players or the beneficial ownership of their funds.

F.5.3 Credit facilities and CCFs

- 206 The matters referred to above in section F.3.1 and paragraphs 189 and 198 are repeated here in relation to the provision of Credit Facilities and CCFs to junket operators or representatives.
- 207 Often, international VIPs would apply for Credit Facilities or CCFs from Crown Melbourne and Crown Perth to fund the purchase of gaming chips. The inherent commercial risk to Crown Melbourne and Crown Perth of non-repayment of gambling debts was amplified for international VIPs who came from jurisdictions in which the enforcement of a gambling debt was practically difficult. Given this, Crown would often decline to offer prospective but unknown international VIPs (ie, those without a reliable debt repayment history with Crown or another casino, or new gaming patrons) gaming chips on credit, as Crown could not be satisfied as to their creditworthiness. Where this issue emerged, Crown Melbourne and Crown Perth would seek to direct these customers to participate in gambling through platform junkets, with Crown extending the credit to the platform junket (as defined in paragraph 67 above). Platform junkets generally referred to larger, more credit-worthy junkets and collections of debts from these junkets were considered by Crown Melbourne and Crown Perth to carry lower credit risk than direct collections from international VIP customers. However, there was a lack of transparency and level of anonymity created by the pooling of all players' funds and transactions, including any CCFs or Credit Facilities provided to the junket operator, under the name of the junket operator.

F.5.4 Remittance

- 208 In the Relevant Period, Crown Melbourne and Crown Perth provided remittance services (items 31 and 32, table 1, section 6 of the AML/CTF Act) through junket channels.
- 209 Junket operators and junket representatives were permitted to transfer money from DABs in their names to DABs in the names of:
- (a) other persons, including other junket operators and representatives; and
 - (b) third parties who were not associated with the junket.
- 210 Crown's policy was that junket operators and junket representatives could transfer money from DABs in their names to DABs in the name of a junket player when the funds transferred were consistent with or matched the junket player's gaming activity as recorded under the relevant junket program. However, the Standard Part A Program did not include appropriate systems or controls for Crown to reliably ascertain and verify whether transfers between DABs were consistent with gaming activity by junket players.
- 211 Crown Melbourne and Crown Perth also facilitated third party telegraphic transfers of funds to and from DABs held by junket operators and representatives, including from junket players and from other persons who were not associated with the relevant junket program. Crown Melbourne and Crown Perth facilitated the payment of junket player winnings in reliance upon records maintained on Crown's SYCO casino management system that were derived from junket operator records and key player ratings. Junket player winnings could be transferred from a junket operator's DAB by telegraphic transfer to either the junket player or another third party. For example, in February 2017, \$100,000 was transferred from Customer 1's Crown Melbourne

DAB to a third party with a comment stating that the winnings were from a key player, Customer 20.

- 212 The Standard Part A Programs did not include appropriate controls to identify, mitigate and manage the ML/TF risks associated with providing remittance services through junket channels for the following reasons:
- (a) at no time did Crown Melbourne or Crown Perth appropriately identify and assess the ML/TF risks of transactions on DABs held by junket operators or representatives;
 - (b) records of winnings by junket players were unreliable because there was a lack of transparency and level of anonymity by the long and complex value chains associated with the flows of junket-related funds, the pooling of all players' funds, credit and transactions under the name of the junket operator;
 - (c) at no time did Crown Melbourne or Crown Perth appropriately assess the ML/TF risks of providing items 31 and 32, table 1, section 6 of the AML/CTF Act designated services to junket operators, representatives or players through higher-risk channels including the Southbank and Riverbank accounts and the Suncity account. An external auditor identified transfers through the Southbank and Riverbank accounts from junket operators to 136 beneficiaries who were not recorded by Crown Melbourne or Crown Perth as players on junkets operated by those individuals. These transactions amount to a total of AUD\$134,721,037 and HKD\$38,637,044; and
 - (d) prior to November 2020, the Standard Part A Programs did not include appropriate operational controls to limit or mitigate and manage the ML/TF risks of third party transfers and/or deposits. For example, from 1 March 2016, Crown Melbourne reported as suspicious approximately \$23 million worth of telegraphic transfers to and from Customer 1's DAB.²⁰

F.5.5 Cash transactions, private gaming rooms and cash administration desks

- 213 Between March 2016 and March 2020, junket operators had arrangements with junket players whereby cash could be advanced to the junket players (or their travel companions) for use while on their visit to Australia, such as for shopping, dining or admission tickets at tourist attractions. Money advanced on this basis would typically have been accounted for when the junket settled their winnings or losses accrued during the junket program with the junket player. Sometimes cash was paid to a junket player by a junket operator in exchange for chips held by the player - in effect cashing in the chips.
- 214 In order to facilitate play under junket programs, Crown Melbourne and Crown Perth made private gaming rooms available to certain junkets on either an exclusive basis (as was the case for the Suncity junket, which had access to a private gaming room in Crown Melbourne on an exclusive basis between February 2014 and August 2019) or a non-exclusive basis (as was the case for the remainder of private gaming rooms made available to junket programs at Crown Melbourne and Crown Perth, including the Suncity junket's use of a Crown Melbourne private gaming room from August 2019 until March 2020).
- 215 From February 2014 to March 2020 (after which the casino was closed due to the COVID-19 pandemic), Crown Melbourne allowed the Suncity junket to operate a cash administration desk in two private gaming rooms, Pit 38 and Pit 86, which was serviced by Suncity staff (**Suncity**

Room). During this period, Crown Perth made private gaming rooms available to the Suncity junket on a non-exclusive basis.

216 Further:

- (a) from 1 March 2016 to March 2020, Crown Melbourne made a villa in Crown Towers available to representatives of the Song junket from time to time. From time to time, this villa was also used by persons associated with the Chinatown junket;
- (b) from April 2018 to March 2020, Crown Melbourne made a cash administration desk available to the Meg-Star junket in private gaming rooms. Meg-Star junket staff members dispensed commission chips in exchange for cash to junket players. Between 9 and 14 April 2018, Crown Melbourne permitted cash-outs of up to \$3 million through this desk; and
- (c) until March 2020, Crown Perth provided the junket operator known as Person 36 with non-exclusive access to a private gaming room. Person 36 was permitted to operate an administration desk to facilitate and record the number and value of gaming chips that were distributed to, and received back from, each junket player.

217 Private gaming rooms, including cash administration desks, were channels through which Crown Melbourne and Crown Perth provided designated services.

218 From 1 March 2016 to March 2020, the provision of designated services to junkets by Crown Melbourne and Crown Perth in private gaming rooms posed higher ML/TF risks:

- (a) From 1 March 2016 to December 2018, there were at least 75 suspicious 'incidents' in the Suncity Room, known to Crown Melbourne, involving cash transactions totalling approximately \$23 million. These incidents involved suspicious activity, including cash brought into the Suncity Room by unknown persons; cash being exchanged between junket representatives and unknown persons in the Suncity Room; and cash being carried in suitcases, envelopes, Crown carry bags, brown paper bags or shoe boxes. For example, during this time, Customer 24 was identified in CCTV footage handing out money from a cooler bag full of cash. A year later, they were arrested in the Suncity Room in connection to a money laundering investigation;
- (b) In the six months prior to May 2018, Crown Melbourne gave the AUSTRAC CEO 58 SMRs concerning behaviour in the Suncity Room, relating to transactions totalling \$16.8 million. By no later than June 2018, the Chief Legal Officer of Crown Resorts, who was also the AMLCO for both Crown Melbourne and Crown Perth, was briefed on the suspicious activity in the Suncity Room;
- (c) Customers, some of whom were not players on Suncity junkets, including Customer 22 (see paragraph 230 below), transacted at the Suncity cash administration desk, often with large amounts of cash. For example:
 - (i) In November and December 2017, Customer 20 exchanged at least \$1 million in cash for chips at the Suncity cash administration desk, often not playing afterwards;
 - (ii) Between October 2017 and March 2018, Customer 23 deposited approximately \$760,000 in cash at the Suncity cash administration desk;

- (iii) Between December 2017 and August 2018, Customer 25 deposited over \$1 million in cash at the Suncity cash administration desk, often in denominations of \$100 and \$50 notes; and
 - (iv) Between October 2018 and December 2018, there were a series of suspicious cash transactions involving five identical cash deposits of \$200,000 presented in \$50 notes from third parties into Customer 1's DAB. A number of individuals who made the deposits claimed that they got the cash from home; and
 - (d) Crown Melbourne received at least three separate enquiries from law enforcement agencies in 2018 relating to the Suncity cash administration desk, including:
 - (i) two in respect of cash deposits of \$700,000 and \$5.6 million in April 2018; and
 - (ii) one inquiry in December 2018 in respect of an incident where a Suncity employee handed Customer 23 a backpack containing at least \$250,000 cash in the Crown Melbourne parking area. The backpack was found to have been taken from the Suncity Room.
- 219 The Standard Part A Programs did not include appropriate controls to identify, mitigate and manage the ML/TF risks associated with the provision of designated services through private gaming rooms and cash administration desks within private rooms for the following reasons:
- (a) neither Crown Melbourne nor Crown Perth carried out an appropriate ML/TF risk assessment with respect to the risks associated with private gaming rooms and cash administration desks within private gaming rooms for junket operators, including with respect to the Suncity, Meg-Star and Person 36 cash administration desks;
 - (b) Crown Melbourne had little visibility over transactions conducted through the Suncity cash administration desk and the Meg-Star cash administration desk. Crown Melbourne does not know whether or not designated services were provided through the villa made available to the Song junket;
 - (c) Crown Melbourne did not make or keep appropriate records in relation to transactions in the Suncity Room, including cash transactions facilitated through the Suncity cash administration desk. Nor did Crown Melbourne make or keep appropriate records in relation to transactions facilitated through the Meg-Star cash administration desk, or of transactions in the Song villa;
 - (d) controls to address ML/TF risks of providing designated services in gaming rooms occupied by junkets, including monitoring of transactions within private gaming rooms, were generally limited to surveillance and identifying junket players and their guests prior to entry into the room. In particular, until April 2018, Crown Melbourne's records of cash transactions conducted at the Suncity cash administration desk were limited to manual surveillance. The Standard Part A Programs did not apply appropriate risk-based transaction monitoring in the Suncity Room;
 - (e) neither Crown Melbourne nor Crown Perth carried out appropriate due diligence with respect to the junket operators who were permitted to operate junkets in private gaming rooms; and
 - (f) Crown Melbourne staff were not adequately trained on ML/TF risks and AML/CTF controls.

- 220 From April 2018, in recognition of the heightened ML/TF risks associated with the use of high volumes of cash in the Suncity Room and junkets more generally, Crown Melbourne introduced various controls that were designed to manage and mitigate those risks:
- (a) from April 2018, Crown Melbourne required all cash transactions in the Suncity Room to be conducted through the Crown Melbourne Cage and not the Suncity cash administration desk, other than for petty cash transactions up to \$100,000. However, after April 2018, on some occasions petty cash was paid to junket players through the Suncity cash administration desk in exchange for chips, notwithstanding this control;
 - (b) in July 2018, Crown Melbourne relocated the Suncity Room to Pit 38. Pit 38 was within the Mahogany Room, at a location where enhanced access controls were in place to ensure that all persons entering the Suncity Room were identified and recorded in Crown Melbourne's system. These further controls were maintained when the Suncity Room was relocated back to Pit 86 in March 2019. However, at no time was there a process to verify the identification presented by customers or guests;
 - (c) from November 2018, a \$300,000 cap on cash transactions in any 24 hour period was introduced at Crown Melbourne for junket operators, junket representatives and key players; and
 - (d) from December 2018, Crown Melbourne required that any bag taken into the Suncity Room be transparent so that video surveillance could monitor the contents of bags when individuals entered and exited the Suncity Room.
- 221 While these measures improved the control environment in which the ML/TF risks relating to large cash transactions associated with junkets and large sums of cash being brought into and out of the Suncity Room were mitigated and managed, they did not go far enough.

F.5.6 Due diligence

- 222 Junket operators, junket representatives and junket players were subject to the same due diligence requirements and screening checks required by the Standard Part A Programs that applied to other Crown Melbourne and Crown Perth customers.
- 223 In addition to these requirements, Crown Melbourne and Crown Perth conducted additional due diligence for prospective junket operators before entering into a relationship with the junket operator. This due diligence did not appropriately identify, mitigate and manage the higher ML/TF risks with respect to designated services provided through the junket channel, in that:
- (a) junket representatives were not subject to any additional due diligence over and above the due diligence controls and screening checks that applied to all customers;
 - (b) appropriate records of due diligence on junket operators were not kept, and ECDD was not consistently recorded in Crown's customer management system;
 - (c) the initial due diligence carried out in respect of junket operators was performed by the Credit Control team and the annual reviews of Crown's relationships with junket operators were carried out within the VIP International business. Neither the initial due diligence nor the annual reviews gave appropriate consideration to the ML/TF risks associated with each junket operator;
 - (d) due diligence was conducted only on the individual who applied for approval to become a junket operator. Where the individual was associated with a corporate entity relevant to

the individual's junket operations, Crown did not conduct appropriate due diligence on the corporate entity; and

- (e) in circumstances where there were reasonable grounds to consider that the junket operator and the individual or entity financing the junket were not one and the same, or that another individual or entity had financial interests in the operations of the junket, Crown did not take appropriate steps to understand the junkets' source of funds, or carry out appropriate due diligence on junket financiers who underwrote credit lines for the junket operators.

F.5.7 ML/TF risks of designated services provided to junkets, including platform junkets

224 On and from 1 March 2016 until August 2020, Crown Melbourne and Crown Perth provided designated services to several junket operators who operated platform junkets. The junket operators and number of junket programs were as follows:

- (a) Customer 1, who was the operator of the Suncity junket. In November 2021, Customer 1 was arrested in a foreign country in connection with allegations relating to an illegal gambling syndicate and money laundering. Crown Melbourne and Crown Perth facilitated 252 Suncity junket programs, the turnover of which exceeded \$22.2 billion between 1 March 2016 and late 2020;²¹
- (b) Customer 2, who was the operator of the Song junket. Crown Melbourne and Crown Perth facilitated 72 Song junket programs. The turnover of the Song junket was approximately \$10.6 billion by no later than March 2020;²²
- (c) Customer 3, who was the operator of the Meg-Star junket. Crown Melbourne and Crown Perth facilitated 268 Meg-Star junket programs. The total turnover of Meg-Star junket programs from December 2014 to late 2020 was approximately \$10.7 billion;²³
- (d) Person 3 and Customers 6 - 9, who formed a network of junket operators affiliated with the Neptune junket. For example, between FY2016 and FY2020, Customer 6 operated at least 123 Neptune junket programs with total turnover which exceeded \$11 billion;²⁴ and
- (e) Customers 10 - 14 formed a network of junket operators affiliated with the Chinatown junket. Crown Melbourne and Crown Perth facilitated at least 52 Chinatown junket programs. Between FY2016 and FY2020, Customer 11, Customer 12 and Customer 14 operated Chinatown junket programs the turnover of which was approximately \$4.7 billion.²⁵

225 Each of these junket operators posed high ML/TF risks:

- (a) designated services provided by Crown Melbourne and Crown Perth to these junket operators involved the ML/TF risks set out at paragraph 71;
- (b) Customers 1 and 3 were foreign PEPs at all times on and from 1 March 2016. Crown Melbourne rated Customer 1 as a foreign PEP on 5 June 2017, and Customer 3 as a foreign PEP on 5 April 2017. Neither customer was rated as a foreign PEP by Crown Perth;

²¹ For an explanation of turnover and its relationship to revenue and profit, see paragraphs 61 to 65.

²² For an explanation of turnover and its relationship to revenue and profit, see paragraphs 61 to 65.

²³ For an explanation of turnover and its relationship to revenue and profit, see paragraphs 61 to 65.

²⁴ For an explanation of turnover and its relationship to revenue and profit, see paragraphs 61 to 65.

²⁵ For an explanation of turnover see paragraphs 61 to 62.

- (c) Customers 1, 2, 3, 6, 7, 8, 9, 10, 11, 12, 13 and 14 were connected to other Crown Melbourne or Crown Perth customers in respect of whom Crown Melbourne or Crown Perth had formed suspicions. Crown Melbourne and Crown Perth gave the AUSTRAC CEO more than 600 SMRs relating to Customers 1, 2, 3 and 6 to 14 from 1 March 2016;
- (d) Customers 10, 11, 12, 13 and 14 were known by Crown Melbourne and Crown Perth to be operating junkets that were financed by third parties, or in which third parties had a financial interest. For example, Crown Melbourne and Crown Perth understood Person 41 to be a likely ultimate beneficial owner of the Chinatown junket with financial interests in its operations. Crown was also aware of information indicating Person 41 was connected to organised crime, including money laundering. Throughout the Relevant Period, Crown received a number of requests for information from law enforcement agencies relating to Person 41, some of which related to their alleged involvement in laundering money for organised crime groups. Further, by August 2019, Crown was aware of media reports that Person 41 was involved in a criminal multi-million dollar fraud scheme. In addition to Person 41, Crown also understood that likely third party ultimate beneficial owners of the Chinatown junket comprised Person 41's spouse, Person 25 and Person 25's spouse;
- (e) Customers 1, 2, 3, 6, and 14 engaged in transfers of large values to or from other Crown Melbourne or Crown Perth customers in circumstances where Crown Melbourne or Crown Perth were not aware of, or did not understand, the connection between these customers. For example, in December 2016, Customer 6 arranged for \$4,000,000 to be transferred from their Crown Perth DAB to Customer 1's Crown Melbourne DAB;
- (f) Customers 1, 2, 3, 6, 11 and 14 engaged in large financial transactions with unknown domestic or international third parties, including overseas remitters (in the case of two customers);
- (g) Customers 1, 2 and 3 transacted using Crown Patron Accounts, often with individual and corporate third parties located overseas. For example, in October 2019, Customer 2 received four payments from third parties through the Southbank account totalling \$300,000²⁶ and in February 2018, Customer 3 received a payment of \$1 million from a third party into the Southbank account;
- (h) Customer 2 used the COD service. Their junket representative arranged for a cash deposit of HKD10,000,000 at the COD for the purpose of discharging Customer 2's credit marker owed to Crown Melbourne;
- (i) Customers 1, 2, 3, 6, 7, 8, 9, 11 and 14 engaged in transactions indicative of ML/TF typologies and vulnerabilities at Crown Melbourne and Crown Perth. Further, some junket players playing on the junkets of platform junket operators engaged in transactions indicative of ML/TF typologies and vulnerabilities at Crown Melbourne and Crown Perth;
- (j) Customers 1, 2, 3, 6 and 14 transacted with large amounts of cash and cash that appeared suspicious. For example, on 24 December 2017, Customer 6's junket representative withdrew \$600,000 in cash from Customer 6's DAB and refused to answer when asked what the funds were for. In February 2018, Customer 14's junket representatives withdrew \$2 million in cash, and deposited \$500,000 in cash, from their DAB. In January 2018, Customer 2's junket representative presented over \$800,000 in

cash that appeared suspicious, including bundles of \$50 notes and notes wrapped in plastic;

- (k) Crown Melbourne provided Customers 1, 2, 6 and 7 with access to the private jet to facilitate both domestic and overseas travel. In February 2018, Customer 6 was discovered to be in possession of \$790,000 in undeclared cash on Crown's private jet;
- (l) on and from 1 March 2016, Crown Melbourne and Crown Perth were aware of information suggesting that the platform junket operators were connected to organised crime or that their source of funds/wealth may otherwise not be legitimate. For example, by late December 2016, Crown Melbourne and Crown Perth became aware that funds from Customer 2's DAB were the subject of proceeds of crime proceedings in Victoria in 2016 on the basis of suspected money laundering and tax avoidance;
- (m) the platform junket operators were known to be connected to other Crown Melbourne or Crown Perth customers including:
 - (i) customers in respect of whom Crown Melbourne or Crown Perth had formed suspicions. For example, between 26 December 2019 and 2 January 2020, Customer 1 received \$900,000 from Customer 20. Between April and December 2019, Crown Melbourne had given the AUSTRAC CEO 27 SMRs in respect of Customer 20. During this period, Crown Melbourne gave the AUSTRAC CEO 17 SMRs in respect of Customer 20; and
 - (ii) customers in respect of whom Crown Melbourne or Crown Perth were aware of information suggesting that they were connected to organised crime or that their source of funds/wealth may otherwise not be legitimate. For example, in July 2019, Crown became aware that Customer 26, a junket representative of Meg-Star and also connected to the Suncity junket, was a brothel owner who was allegedly linked to organised crime and allegedly engaged in human sex trafficking. By 2014, Crown had received inquiries from law enforcement about Customer 26 in connection with alleged sex offences, possible operation of illegal brothels and using Crown for money laundering; and
- (n) Customers 1, 2, 3, 6, 9, 11, 12 and 13 received large amounts of credit from or after 1 March 2016 with limits ranging from \$20 million (Customer 2 in March 2016 and Customer 9 in March 2018) to \$140 million (Customer 12 in July 2016 and Customer 13 in October 2016).

226 Further, on and from 1 March 2016 until August 2020, Crown Melbourne and Crown Perth provided designated services to junket representatives and players, and several non-platform junket operators which also posed high ML/TF risks:

- (a) designated services provided by Crown Melbourne and Crown Perth to these junkets involved the ML/TF risks set out at paragraph 71;
- (b) a number of junket operators, junket representatives and junket players were foreign PEPs;
- (c) junket customers were often connected to other Crown Melbourne or Crown Perth customers in respect of whom Crown Melbourne or Crown Perth had formed suspicions;

- (d) some customers were connected to multiple junkets, often concurrently. Junket operators sometimes also played on their own junkets or through other junkets. For example, Customer 19 turned over approximately \$44.8 million playing on their own junkets;²⁷
- (e) junket customers engaged in transfers of large values to or from other Crown Melbourne or Crown Perth customers in circumstances where Crown Melbourne or Crown Perth were not aware of, or did not understand, the connection between these customers;
- (f) junket customers engaged in large financial transactions with domestic or international third parties, including overseas remitters. For example, Customer 4 received over \$36 million via a money remitter between December 2017 and May 2018, and over \$70 million from an individual third party in the period from June 2017 to February 2020. Customer 18 received approximately \$16 million via a foreign remittance service between August and September 2018, \$13 million of which was used as front money for a junket program;
- (g) junket customers engaged in large financial transactions with corporate entities that were often located overseas. For example, Customer 4 received over \$19.5 million worth of deposits from an overseas-based company in a one year period between March 2017 and February 2018;
- (h) junket customers engaged in transactions involving large amounts of cash, often with cash that appeared suspicious. For example, in November 2017, Customer 20 presented at the Suncity cash administration desk with two shopping bags containing approximately \$300,000 in \$100 notes which they exchanged for gaming chips and did not play after the transaction;
- (i) junket customers transferred funds using overseas deposit services and remittance services. Customer 5 transacted over \$3.5 million through this channel, including a \$500,000 transfer via Company 10 as part of an offsetting arrangement to repay a junket debt at Crown Perth. In 2017, Crown Melbourne received a telegraphic transfer of \$1 million for the benefit of Customer 16 from Company 10, to be used as front money;
- (j) junket customers transacted using Crown Patron Accounts, often with unknown third parties. For example, Customer 15 received over \$5.5 million via the Southbank account over a four month period in 2016. Between September 2017 and December 2017, Customer 16 received over \$2 million via the Riverbank account from third parties;
- (k) junket operators often received large CCFs or Credit Facilities from Crown for the purpose of funding junkets. For example, on one occasion Customer 17 was provided with credit up to a limit of \$15 million;
- (l) many junket customers engaged in transactions indicative of ML/TF typologies and vulnerabilities at Crown Melbourne and Crown Perth. For example, over \$15 million of transactions involving Customer 4 between July 2016 and March 2020 were indicative of the ML/TF typology of quick turnover of funds without betting;
- (m) a number of junket operators had parked funds. For example, between 24 November 2020 and 18 June 2021, Customer 4's DAB had a balance of just over \$7 million. On 28 June 2021, Customer 4 was permitted to transfer those funds to an international bank account in their name;

²⁷ For an explanation of turnover and its relationship to revenue and profit, see paragraphs 61 to 65.

- (n) Crown Melbourne and Crown Perth received law enforcement requests with respect to a number of junket customers including Customers 5, 15, 18, 20 and 26. For example, Crown received law enforcement inquiries in relation to Customer 26 regarding possible operation of illegal brothels and using Crown for money laundering. Further, Crown was aware of law enforcement enquires involving Customer 5 on two occasions in 2017 in relation to the origin of cash presented in plastic bags; and
 - (o) Crown Melbourne and Crown Perth were aware that a number of junket customers, including Customer 24 had been arrested in connection with money laundering investigations. Customer 24 was arrested in Pit 86 at Crown Melbourne in 2018.
- 227 Some customers transacted through multiple junkets, including platform junkets, at the same time. The controls in Crown's Standard Part A Programs were not capable of identifying, mitigating and managing unusual or suspicious activity across multiple junkets.
- 228 In view of these circumstances, and the higher ML/TF risks associated with the provision of designated services through the junket channel as described in paragraph 71 above, the Standard Part A Programs did not include appropriate risk-based controls to identify, mitigate and manage the higher ML/TF risks posed by designated services provided through junkets.
- 229 A limited number of former junket representatives have returned to Crown Melbourne and, having been cleared through the Significant Player Review process, have been permitted to play as regular customers.

F.5.7.1 Junket risk case study: Customer 22

- 230 During the period December 2017 to January 2018, Customer 22 was involved in a number of transactions at the Suncity cash administration desk that appeared suspicious and which involved the movement of over \$1.9 million. For example, on 1 January 2018, Customer 22 made seven deposits of cash at the Suncity cash administration desk totalling \$495,000 over the course of less than 4 hours: \$100,000, \$80,000, \$60,000, \$60,000, \$85,000, \$50,000, and \$60,000.
- 231 Customer 22 was also involved in transactions in connection with the Song junket, operated by Customer 2. In January 2018, Customer 2's junket representatives engaged in large cash transactions on behalf of third parties, including Customer 22. Crown Melbourne gave SMRs to the AUSTRAC CEO in January 2018 which recorded suspicions of Customer 22's involvement in the movement of \$620,000 in cash in connection with the Song junket.
- 232 Customer 22 was a customer of Crown Melbourne from June 2015 to September 2021 (but had no rated play in 2019-2021). In addition to connections to Customer 1, the Suncity junket, Customer 2 and the Song junket, Customer 22 was also known to be connected to Customer 26, a junket representative for Meg-Star, who had alleged connections to human sex trafficking and who was issued a withdrawal of licence (**WOL**) by Crown Melbourne for signing excluded customers into a private gaming room. For example, in January 2018, Customer 26 cashed out \$687,000 and gave the cash in a bag to Customer 22.
- 233 From November 2017, provision of designated services to Customer 22 involved factors that posed higher ML/TF risks including: large transfers to and from third parties; movement of funds through Southbank and Riverbank accounts; and transacting with large amounts of cash and cash that appeared suspicious, including large volumes of cash in carry bags and plastic bags. In 2015-2018, Customer 22 made 97 incoming cash transactions totalling \$5,736,800 and 288 outgoing cash transactions totalling \$13,015,428.

- 234 In the course of a transactional lookback by an independent auditor in 2021, transactions indicative of ML/TF typologies were identified with respect to Customer 22, including: possible attempts to layer funds; use of cash, multiple bank accounts, inconsistent narratives and third parties, which could be an attempt to disguise the source of the funds; quick turnover (without betting); parked funds; use of third party agents; and cash withdrawals that did not align with gaming or deposit data.
- 235 For example, from April to June 2017, Customer 22 made cash withdrawals totalling over \$1 million each month. Crown Melbourne gave the AUSTRAC CEO 20 SMRs between 27 March 2017 and 29 November 2021 with respect to Customer 22. Customer 22 was not rated high risk until August 2021. Prior to the decision to issue Customer 22 with a WOL, there is no record of senior management considering whether to continue doing business with Customer 22. During the period 2017-2018, Customer 22 was associated with approximately \$698.5 million in turnover²⁸, and transactions totalling over \$18 million which were identified in a 2021 lookback conducted by an independent auditor as transactions indicative of ML/TF risk.

F.6 Transaction monitoring programs

- 236 At all times during the Relevant Period, Crown Melbourne and Crown Perth were required to have a TMP that complied with the requirements described in Section D above.

F.6.1 Crown Melbourne's TMP

- 237 Between 1 March 2016 and 1 November 2020, Crown Melbourne's TMP was set out in clause 12 and Annexure F of the Crown Melbourne Standard Part A Program:
- (a) Clause 12 in each version of the Crown Melbourne Standard Part A Program provided that the CTRM (or, in version 8, the AML Team) would monitor the following transactions to detect materially abnormal transaction values or other behaviours that suggested higher than usual ML/TF risks:
 - (i) cash transactions of \$10,000 or more;
 - (ii) cheques issued to customers;
 - (iii) buy-ins (carded, uncarded, voided);
 - (iv) account opening and transacting;
 - (v) foreign currency transactions;
 - (vi) trends in play;
 - (vii) cancelled credits and jackpots on EGMs;
 - (viii) Centrelink concession cardholder (to the extent known);
 - (ix) names of known customers in government reports of persons becoming bankrupt or deceased; and
 - (x) names of known customers in World Check.
 - (b) Clause 12 in version 8 of the Crown Melbourne Standard Part A Program further provided that the AML Team would monitor the following to detect materially abnormal transaction values or other behaviours that suggested higher than usual ML/TF risks:
 - (i) customer behaviours;

²⁸ For an explanation of turnover and its relationship to revenue and profit, see paragraphs 61 to 65.

- (ii) activity on EGMs and ETGs over a gaming day; and
 - (iii) TITO tickets with a value of more than \$5,000 aged more than 24 hours.
 - (c) Clause 12 and Annexure F in each version of the Crown Melbourne Standard Part A Program identified the methods for monitoring the activities and attributes described in (a) and (b) above, which included manually reviewing system-generated transaction activity reports, data matching and staff observation. Annexure F in each version of the Crown Melbourne Standard Part A Program identified the frequency for generating transaction activity reports, which was either periodic (daily, weekly, quarterly or yearly) or as required.
 - (d) Clause 12 in each version of the Crown Melbourne Standard Part A Program stated that transaction activity reports had to be considered by the CTRM (or, in version 8, the AML Team) with a view to cross-matching data and generally looking for a rational basis to lodge an SMR, add information to the ML/TF risk information of a customer, and generally assess ML/TF risk.
- 238 In addition, the Risk Register in each version of the Crown Melbourne Standard Part A Program, although not expressly forming part of the TMP, contained some detective controls to address specific ML/TF risks. These controls usually took the form of staff observation and reporting.

F.6.2 Crown Perth's TMP

- 239 Between 1 March 2016 and 1 November 2020, Crown Perth's TMP was set out in clause 12 of the Crown Perth Standard Part A Program, which incorporated the Crown Perth AML SOPs:
- (a) Clause 12 in each version of the Crown Perth Standard Part A Program provided that the AML Officer (or, from version 16, the Legal Officer – AML) would monitor the following transactions for ML/TF risks:
 - (i) cash transactions equal to or greater than \$10,000;
 - (ii) cheques issued to customers;
 - (iii) buy-ins (carded, uncarded, voided);
 - (iv) account opening and transacting;
 - (v) foreign currency transactions equal to or greater than AU\$1,000;
 - (vi) trends in play;
 - (vii) Centrelink concession cardholder (to the extent known);
 - (viii) names of known customers in World Check; and
 - (ix) until November 2018, names of known customers becoming bankrupt (to the extent known).
 - (b) Clause 12 in versions 16 and 17 of the Crown Perth Standard Part A Program further provided that the Legal Officer – AML would monitor customer behaviour for suspicious matters.
 - (c) Clause 12 in each version of the Crown Perth Standard Part A Program identified the methods for monitoring the activities and attributes described in (a) and (b) above, which included manually reviewing system-generated transaction activity reports, data matching and staff observation. Sections 3.1 to 3.4 of the Crown Perth AML SOPs identified the

frequency for generating transaction activity reports, which was either periodic (daily, weekly, fortnightly, monthly or quarterly) or as required.

- (d) Clause 12 in each version of the Crown Perth Standard Part A Program stated that transaction activity reports had to be considered by the AML Officer (or, from version 16, the Legal Officer – AML) with a view to cross-matching data and generally looking for a basis to lodge a SMR, add information to the ML/TF risk information of a customer, and assess ML/TF risk.

240 In addition, the Risk Register in each version of the Crown Perth Standard Part A Program, although not expressly forming part of the TMP, contained some detective controls to address specific ML/TF risks. These controls usually took the form of staff observation and reporting.

F.6.3 Compliance of TMPs

241 The TMPs in the Crown Melbourne and Crown Perth Standard Part A Programs (together, the **Transaction Monitoring Programs**) did not fully comply with the requirements of paragraphs 8.1.3, 8.1.4 and 15.4 to 15.7 of the AML/CTF Rules for the reasons described in paragraphs 242 to 246 below. As a result, between 1 March 2016 and 1 November 2020, the Crown Melbourne and Crown Perth Standard Part A Programs did not comply with section 84(2)(c) of the AML/CTF Act.

Not aligned to an appropriate ML/TF risk assessment

242 Crown Melbourne and Crown Perth needed to include in their Transaction Monitoring Programs appropriate risk-based systems and controls to monitor the transactions of customers. When determining and putting in place the appropriate risk-based systems and controls, Crown Melbourne and Crown Perth had to have regard to the nature, size and complexity of their businesses, and the types of ML/TF risk they reasonably faced.²⁹ As described in F.1 above, Crown Melbourne and Crown Perth did not appropriately assess the ML/TF risks associated with their provision of designated services. As a result, as described in paragraphs 243 to 246 below, the systems and controls in the Transaction Monitoring Programs were not able to appropriately address the ML/TF risks that Crown reasonably faced across all designated services.

Reliance on manual and observational processes

243 The Transaction Monitoring Programs were reliant on manual and observational processes, which were inadequate, given the nature, size and complexity of Crown's businesses, and the types of ML/TF risks they faced. As operators of casinos, Crown Melbourne and Crown Perth were particularly vulnerable to money laundering. The ML/TF typologies and vulnerabilities addressed in B.6 above, which were applicable to Crown Melbourne and Crown Perth, included complex, unusual large transactions and unusual patterns of transactions that could not have been observed or consistently detected using the manual and observational processes in the Transaction Monitoring Programs. This is because:

- (a) The manual and observational processes were focused on individual transaction sets, and were not capable of consistently detecting suspicious or unusual patterns of transactions or behaviours across complex transaction chains involving multiple designated services.

²⁹ See paragraphs 15 to 17 for an explanation of appropriate risk-based procedures, systems and controls.

- (b) The Transaction Monitoring Programs did not provide adequate review criteria for the system-generated transaction activity reports that were central to the manual processes, nor did they provide adequate guidance on how to identify unusually large transactions. In addition, staff reviewing system-generated transaction activity reports did not receive adequate ML/TF risk awareness training. Nor did the resourcing of the AML/Financial crime function support the consistent generation, review and actioning of systems-generated or exception-based reports.
- (c) The system-generated transaction activity reports that were central to the manual processes were reliant on data accessible from Crown's information management systems. However, the information management systems:
 - (i) were reliant on manual data entry that was susceptible to human error. For example, dealers at tables were required to record manually transaction data into ATOM (a system linked to SYCO) whilst facilitating table games. Therefore, there was a risk that dealers might fail to capture all transactions at table games relating to the provision of designated services;
 - (ii) did not always contain complete records of customer transactions. In particular, Crown's SYCO system had limited records of customer transactions under \$10,000 unless a customer elected to play carded (that is, against a Crown Rewards membership). Therefore, Crown was unable to fully monitor, among other things, transactions structured to avoid threshold transaction reporting;
 - (iii) were not supported by processes for the reliable and consistent entry of KYC information for customers with uncarded transactions of \$10,000 or more, until after October 2020. From October 2020, Table Games staff were required to enter a customer's KYC information into SYCO (Crown Melbourne) or LUI³⁰ (Crown Perth) for uncarded buy-ins of \$10,000 or more, directly at the time of buy-in. Prior to that date other teams were responsible for entering this information into SYCO (e.g. following issue logs or forms containing KYC details being sent to AML by Table Games for completion of a TTR), which created the potential for delays and gaps in data entry; and
 - (iv) were unable to consistently link individual transactions, and patterns of transactions, to the customers engaging in those transactions because:
 - (A) of the issues set out at (i) to (iii);
 - (B) records relating to customers were dispersed across different systems;
 - (C) Crown gave customers more than one gaming account and/or reference number; and
 - (D) Some customers had multiple gaming accounts in different names or pseudonyms.

244 The Transaction Monitoring Programs did not include or incorporate appropriate risk-based automated monitoring, despite Crown Melbourne and Crown Perth both receiving recommendations from AUSTRAC to consider implementing automated transaction monitoring processes in 2012 and subsequently. Crown Melbourne and Crown Perth did not begin work to

³⁰ Loyalty User Interface.

build an automated transaction monitoring solution until 2019, and this solution did not go live until February 2021.

Absence of appropriate monitoring of certain transactions

245 The Transaction Monitoring Programs did not include appropriate risk-based systems and controls to:

- (a) identify transactions that met the transactional criteria in the Crown Melbourne Standard Part A Program requiring that a customer be risk-rated above low risk. Manual and observational processes in the Crown Melbourne TMP could not consistently identify transactions that met these criteria. (There was no transactional criteria in the Crown Perth Standard Part A Program to detect customers who were not low risk);
- (b) monitor transactions associated with junket channels, noting that the customers who received designated services through the junket channels were subject to the same monitoring that was applied to all customers, despite the provision of designated services through the junket channels involving higher ML/TF risks (see sub-paragraph 218(b) for further detail);
- (c) monitor the transactions of customers in relation to designated services on DABs and SKAs under item 13, table 3, section 6 of the AML/CTF Act through the Crown Patron Account channel having regard to the ML/TF risks identified at paragraph 189(b);
- (d) monitor transfers from one customer's DAB to another customer's DAB, so as to consistently identify any transactions that may have been suspicious or unusual;
- (e) monitor the provision of the remittance services described at E3 having regard to their ML/TF risks;
- (f) monitor the provision of items 6 and 7, table 1 designated services (Credit Facilities and CCFs), having regard to their ML/TF risks;
- (g) monitor transactions on EGMs and ETGs, noting that the Crown Melbourne TMP did include monitoring over cancelled credits and jackpots on EGMs, and from 23 November 2018, Crown Melbourne did monitor activity on EGMs and ETGs over a gaming day;
- (h) monitor transactions associated with the Hotel Card channel, noting that no monitoring was conducted on the origin of Hotel Card funds, which became commingled with other funds and transactional activity when credited into a customer's DAB;
- (i) monitor transactions through overseas deposit services, having regard to their ML/TF risks;
- (j) monitor cash deposits and withdrawals through the Card Play Extra accounts;
- (k) monitor foreign currency exchange for the typologies identified at paragraph 189(i) above; and
- (l) have regard to the fact that some customers received designated services in HKD for the purposes of determining whether the customer's transactional activity was unusual.

Absence of assurance processes

246 The Transaction Monitoring Programs did not include or incorporate appropriate assurance processes to ensure that the risk-based systems and controls in the Transaction Monitoring Programs were being applied correctly, were operating as intended and remained appropriate.

- 247 As a result of the matters set out at paragraphs 241 to 246, contrary to the requirements of paragraphs 15.4 to 15.7 of the AML/CTF Rules and section 84(2)(c) of the AML/CTF Act, the transaction monitoring programs were not capable of consistently or fully identifying across all designated services and customers:
- (a) transactions that may have had the indicia of the ML/TF typologies and vulnerabilities set out in Schedule 2;
 - (b) transactions that may have been suspicious for the purposes of section 41 of the AML/CTF Act; and
 - (c) unusually large or unusual patterns of transactions, which had no apparent economic or visible lawful purpose.

F.7 Enhanced Customer Due Diligence Programs

- 248 At all times during the Relevant Period, Crown Melbourne and Crown Perth were required to have an ECDD program that complied with the requirements described in Section D above.

F.7.1 Crown Melbourne

- 249 Between 1 March 2016 and 1 November 2020, Crown Melbourne's ECDD program was set out in clause 15 and Annexure H of the Crown Melbourne Standard Part A Program. In addition, Annexure H of the Crown Melbourne Standard Part A Program stated that the ECDD program comprised elements from the following parts of the Crown Melbourne Standard Program:
- (a) Annexure F, which set out Crown Melbourne's TMP and is described at paragraphs 237 to 238 above;
 - (b) Annexure G, which set out Crown's Melbourne's procedures for risk rating customers and is described at F.1.2 above; and
 - (c) the AUSTRAC Guidelines.
- 250 Clause 15 of the Crown Melbourne Standard Part A Program required that ECDD be undertaken when:
- (a) a suspicion arose that would give rise to a SMR;
 - (b) an identified customer, or their beneficial owner, was allocated a risk rating of significant or high (including when the customer or beneficial owner was a known foreign PEP); or
 - (c) Crown Melbourne was entering into or proposing to enter into a transaction and a party to a transaction was in a prescribed foreign country.
- 251 When ECDD was triggered, Annexure H of the Crown Melbourne Standard Part A Program provided that Crown Melbourne would undertake ECDD measures, including, but not limited to:
- (a) reviewing Crown Melbourne's databases, and where appropriate, seeking information from the customer or from other sources to obtain, among other things, information relating to the customer's occupation or business, their financial position, income or assets available to the customer, and the customer's source of wealth or funds (including the origin of funds);
 - (b) reviewing Crown Melbourne's databases, and where appropriate, taking additional reasonable measures to identify and seek information from the customer or other sources to find out the source of the customer's wealth and funds (or those of the customer's beneficial owners, if any);

- (c) undertaking more detailed analysis of the customer's KYC and beneficial owner information; and
 - (d) seeking senior management approval on whether the relationship with the customer should continue, whether any particular transaction should be processed, and/or whether a designated service should continue to be provided to the customer.
- 252 Annexure H of the Crown Melbourne Standard Part A Program provided that if a customer was a foreign PEP or other high risk PEP, Crown Melbourne had to undertake, at a minimum, the measures identified in sub-paragraphs 251(c) and 251(d) above.

F.7.2 Crown Perth

- 253 Between 1 March 2016 and 1 November 2020, Crown Perth's ECDD program was set out in clause 15 of the Crown Perth Standard Part A Program. Additional guidance and procedures were provided in the Crown Perth AML SOPs.
- 254 Clause 15 of the Crown Perth Standard Part A Program required that ECDD be undertaken when:
- (a) Crown Perth determined under its risk-based systems and controls that the ML/TF risk was high;
 - (b) a designated service was being provided to a customer who was or who had a beneficial owner who was a foreign PEP;
 - (c) a suspicion arose that would give rise to a SMR; or
 - (d) Crown Perth was entering into or proposing to enter into a transaction, and a party to the transaction was physically present in, or was a corporation incorporated in, a prescribed foreign country.
- 255 When ECDD was triggered, clause 15 of the Crown Perth Standard Part A Program provided that Crown Perth would undertake, in regard to the identified ML/TF risk or suspicion, one or more of a list of ECDD measures, including, but not limited to:
- (a) making enquiries with the appropriate department manager to obtain further information on, among other things, the customer's occupation and/or business, and the source of the customer's wealth and funds; and
 - (b) seeking senior management approval for continuing a business relationship with the customer and approval for whether a designated service should continue to be provided to the customer.
- 256 Clause 15 in each version of the Crown Perth Standard Part A Program provided that if the customer was a foreign PEP or other high risk PEP, Crown Perth had to undertake, at a minimum, both measures identified in paragraph 255 above.

F.7.3 Compliance of ECDD Programs

- 257 Between 1 March 2016 and 1 November 2020, the ECDD programs in the Crown Melbourne and Crown Perth Standard Part A Programs (together, the **ECDD Programs**), did not fully comply with the requirements in paragraphs 15.8 to 15.11 of the AML/CTF Rules for the reasons described in paragraphs 258 to 260 below. As a result, between 1 March 2016 and 1 November 2020, the Crown Melbourne and Crown Perth Standard Part A Programs did not comply with section 84(2)(c) of the AML/CTF Act.

Systems and controls to determine when a customer should be referred for ECDD

258 The ECDD Programs identified that ECDD needed to be completed in the circumstances specified in paragraph 15.9 of the AML/CTF Rules. However, the ECDD Programs did not include appropriate systems, controls and procedures to ensure that in each of these circumstances, a customer was escalated for ECDD.³¹ In particular, the ECDD Programs required that ECDD be undertaken when a:

- (a) customer posed a high ML/TF risk, as is required under sub-paragraph 15.9(1) of the AML/CTF Rules. The Crown Melbourne and Crown Perth Standard Part A Programs identified circumstances where a customer could or would be allocated a high risk rating. However, the processes for identifying customers that *actually* posed a high ML/TF risk were inadequate, including because:
 - (i) Under the Part B Programs, customers were automatically rated as low risk for the purpose of ACIP without appropriate consideration given to the ML/TF risk posed by the customer type (for example, junket players and VIPs), as required by paragraph 4.1.3 of the AML/CTF Rules.
 - (ii) The Transaction Monitoring Programs were not capable of consistently identifying and escalating customers engaging in unusual or suspicious transactions.
 - (iii) There were no written processes in place for the Credit/VIP International teams to refer customers to the AML/Financial Crime teams for an ML/TF risk assessment or ECDD when, during the course of a credit risk assessment, high ML/TF risks were identified.
 - (iv) Regular review of customer risk ratings was too infrequent to appropriately identify high risk customers and this process did not involve a referral of the customer for full ECDD.
 - (v) There were no appropriate risk-based written processes to determine in what circumstances further KYC information should be collected or verified in respect of a customer to enable the review and update of KYC information for OCDD purposes (including ECDD), as required by paragraphs 15.2 and 15.3 of the AML/CTF Rules.

In addition, the ECDD Programs did not include appropriate systems, controls or procedures to ensure that customers who had been allocated a high risk rating were escalated for ECDD at appropriate intervals.

- (b) customer, or their beneficial owner, was a foreign PEP, as is required under sub-paragraph 15.9(2) of the AML/CTF Rules. The Crown Melbourne and Crown Perth Standard Programs provided that PEPs could be identified using World Check (an external service provider) or the knowledge of Crown Melbourne and Crown Perth staff. Version 17 of the Crown Perth Standard Program provided that PEPs could also be identified using an equivalent reputable service provider to World Check. However, for the reasons identified in paragraph 108, those screening processes were inadequate. In addition, the ECDD Programs did not include appropriate systems, controls and procedures to ensure that when a customer had been identified as a foreign PEP, the customer was escalated for ECDD. For example, there were no processes in place for

³¹ See paragraphs 15 to 17 for an explanation of appropriate risk-based procedures, systems and controls.

the Credit/VIP International teams to refer customers to the AML/Financial Crime teams for ECDD when, during the course of a credit risk assessment, a customer was identified as a foreign PEP. Nor were there appropriate systems and controls to ensure that the minimum ECDD measures for foreign PEPs identified in paragraph 15.11 of the AML/CTF Rules were undertaken.

- (c) reportable suspicion arose for the purposes of section 41 of the AML/CTF Act, as is required under sub-paragraph 15.9(3) of the AML/CTF Rules. The Crown Melbourne Standard Program provided that the decision on whether a suspicion was reportable ultimately rested with the CTRM (or in version 8, the AML Team). The Crown Perth Standard Program provided that the final submission of SMRs to AUSTRAC was the responsibility of the Legal Officer – AML (or their designee). The CTRM (or the AML Team) in Crown Melbourne and the Legal Officer – AML (or their designee) in Crown Perth were expected to initiate ECDD at the time a reportable suspicion was formed. However, the ECDD Programs did not include appropriate systems, controls and procedures to ensure that this happened, or otherwise, that a reportable suspicion was escalated for ECDD. Relevantly, the unusual activity report workflows were not clearly mapped to the ECDD process, and were instead focused on the raising of an SMR.

Systems and controls relating to undertaking ECDD

259 The ECDD Programs identified the ECDD measures that could be undertaken when ECDD was triggered, including the ECDD measures in paragraph 15.10 of the AML/CTF Rules. However, the ECDD Programs did not include appropriate systems, controls and procedures to ensure that the appropriate ECDD measures were undertaken in each circumstance.³² In particular:

- (a) When ECDD was triggered, the Crown Melbourne ECDD program required the CTRM (or in version 8, the AML Team) to consider a list of ECDD measures, and undertake one or more of those measures appropriate to the circumstances. The Crown Perth ECDD program required that Crown Perth undertake one or more of a list of ECDD measures. The ECDD Programs prescribed minimum ECDD measures that applied if a customer was a foreign PEP or other high risk PEP. However, in all other circumstances, there was no guidance for determining which ECDD measures would be undertaken when ECDD was triggered and the ECDD measures to be undertaken were largely at the discretion of the AMLCO. The staff exercising discretion under the ECDD Programs did not receive adequate AML/CTF training.
- (b) The ECDD Programs did not set out appropriate ECDD measures that were aligned to the nature, size and complexity of Crown Melbourne's and Crown Perth's business, and the ML/TF risks posed by customers.
- (c) The ECDD Programs did not include appropriate procedures to ensure analysis of the full suite of designated services received by customers across multiple transaction chains and channels, including designated services provided under table 1, section 6 of the AML/CTF Act.
- (d) The ECDD Programs did not include appropriate procedures to ensure analysis of third-party transactions.

³² See paragraphs 15 to 17 for an explanation of appropriate risk-based procedures, systems and controls.

- (e) The ECDD Programs did not include appropriate procedures to ensure that KYC information would be clarified and verified, beyond re-performing standard KYC checks.
- (f) The ECDD Programs identified, as an ECDD measure, that Crown obtain and analyse source of wealth and source of funds information. The Crown Melbourne ECDD program provided that, in order to obtain source of wealth and source of funds information, Crown Melbourne had to use its databases and, where appropriate, seek information from the customer or other sources. The Crown Perth ECDD program provided that, in order to obtain source of wealth and source of funds information, Crown Perth had to make enquiries with the appropriate department manager. However, the ECDD Programs did not include appropriate systems, controls and procedures to ensure that source of wealth and source of funds information was obtained, analysed and recorded for the purposes of conducting this ECDD measure. For example:
 - (i) The ECDD Programs did not specify what source of wealth or source of funds checks should be conducted, and there was no guidance or criteria for the relevant employees to appropriately analyse the information.
 - (ii) There were no written processes to ensure that source of wealth and source of funds information obtained by VIP International or the International Commission Business for the purposes of credit risk assessments were referred, on a risk basis, to the AML/Financial Crime teams for the purposes of ECDD.
 - (iii) The Standard Part A Programs did not include appropriate risk-based controls to identify customers whose source of wealth or source of funds was unexplained or possibly illegitimate, and in such cases, to determine whether specific transactions should be processed or an ongoing relationship with the customer was within risk appetite.
 - (iv) In the absence of appropriate guidance about source of wealth and source of funds, Crown Melbourne and Crown Perth were unable to carry out appropriate risk-based ECDD measures where source of funds or source of wealth checks were required. For example, Crown Melbourne and Crown Perth were not in a position to understand fully the purpose of customer transactions, or the ML/TF risks they posed. Nor were they in a position to determine appropriately the ML/TF risk posed by the customer and the ongoing business relationship.
- (g) The ECDD Programs identified, as an ECDD measure, that Crown obtain senior management approval for continuing a business relationship with a customer, and whether a designated service should be provided to a customer. However, the ECDD Programs did not include appropriate systems, controls and procedures to:
 - (i) ensure that customers were escalated to senior management for approval when required.
 - (A) All employees were able to escalate customers to the Person of Interest Committees (**POI Committees**), who made decisions on whether customers that were identified as posing a high ML/TF risk should be allowed to continue to frequent the casinos. However, until October 2020, there were inadequate written procedures regarding those escalations.
 - (B) In addition, the Crown Melbourne Standard Program provided that in the case of a foreign PEP, for the purpose of seeking senior management

approval, the AML Team was authorised to make a decision at first instance after consideration of all available information and having regard to the ML/TF risks. The Crown Melbourne Standard Program also provided that the AML Team could refer the final decision to the AMLCO or other members of senior management where appropriate. It was not appropriate for the AML Team to have this discretion, having regard to the nature, size and complexity of Crown Melbourne's business, and the ML/TF risks that foreign PEPs posed.

- (ii) assist senior management in determining whether Crown Melbourne or Crown Perth should continue a business relationship with a customer, or continue to provide a designated service to a customer.
 - (A) It was not until October 2020 that an appropriate set of criteria was established for the POI Committees to make a decision from an ML/TF risk perspective on whether a customer should be allowed to continue to frequent the casinos, or whether an ongoing relationship with the customer was outside of Crown's risk appetite.
 - (B) In addition, Crown Melbourne and Crown Perth had processes for banning individuals from their casinos (the issuance of a WOL, or a notice revoking licence (**NRL**), respectively).³³ However the attendant processes were not attuned to ML/TF risk and did not contain appropriate criteria for making the decision from an ML/TF risk perspective.
 - (C) To the extent that senior management within the VIP International or Credit Control teams considered whether to provide designated services to a customer (such as a loan) or whether to continue an ongoing business relationship, decisions were made from the perspective of credit risk, not ML/TF risk.

Information management and records

260 The ECDD Programs were not supported by appropriate information management and record keeping.³⁴ In particular:

- (a) the Standard Part A Programs did not include appropriate processes to ensure that customer information was consistently entered into the appropriate information management systems when necessary. For example, Crown Melbourne and Crown Perth intended to store KYC information on LUI/CC2 from November 2016, however, the system was not used until October 2019, and when it was used, there were no appropriate processes to ensure the customer information was in fact entered consistently;
- (b) the Standard Part A Programs did not include appropriate processes to facilitate the use of the appropriate information management systems in completing ECDD;
- (c) for the reasons described in paragraph 243(c)(iv), Crown Melbourne and Crown Perth did not have a full view of customers' transactions for ECDD purposes; and

³³ The withdrawal of licence and the notice revoking licence were the decision by Crown Melbourne or Crown Perth respectively to issue a notice revoking the common law licence for a specific customer to enter the casino premises.

³⁴ See paragraphs 15 to 17 for an explanation of appropriate risk-based procedures, systems and controls.

- (d) Crown Melbourne and Crown Perth did not consistently keep records of risk information for the purposes of ECDD, and records of customer risk assessments, ECDD or credit risk assessments were stored on local drives and shared via email, rather than being held in a central repository.

F.8 Reporting obligations

E.8.1 Crown Melbourne

Suspicious matter reporting

261 Between 1 March 2016 and 1 November 2020, the Crown Melbourne Standard Program:

- (a) required Crown Melbourne to report suspicious matters in accordance with section 41 of the AML/CTF Act;
- (b) required that staff complete the AML/CTF online training module, at least once every two years;
- (c) provided for a dedicated officer that was responsible for the management and continuous improvement of Crown's AML/CTF obligations, including monitoring of gaming activity for the identification and reporting of suspicious matters to AUSTRAC; and
- (d) included a number of specific controls that required the reporting of suspicious matters with respect to specific scenarios arising from the designated services provided by Crown Melbourne.

262 Between 1 March 2016 and 1 November 2020, the Crown Melbourne Guidelines:

- (a) provided some guidance on the types of transactions and/or incidents that may require an SMR to be submitted to AUSTRAC;
- (b) provided some guidance (including examples) in relation to some activities which may require an SMR to be submitted to AUSTRAC;
- (c) provided information on obtaining and completing the necessary forms to submit an SMR to AUSTRAC;
- (d) required Crown Melbourne to submit SMRs to AUSTRAC within:
 - (i) 3 business days after the day on which the reporting entity formed the relevant suspicion; or
 - (ii) 24 hours after the time when the reporting entity formed the relevant suspicion if in relation to financing of terrorism; and
- (e) required all SMRs be reviewed and assigned an identifying number by the CTRM prior to submission to AUSTRAC.

Threshold Transaction Reporting (TTRs)

263 Between 1 March 2016 and 1 November 2020, the Crown Melbourne Standard Program:

- (a) required Crown Melbourne to report threshold transactions in accordance with section 43 of the AML/CTF Act;
- (b) required staff to complete training on TTR obligations under the AML/CTF Act and AML/CTF Rules, at least once every two years; and

- (c) included a number of specific controls that required the reporting of threshold transactions in relation to specific scenarios associated with the designated services provided by Crown Melbourne.

264 Between 1 March 2016 and 1 November 2020, the Crown Melbourne Guidelines:

- (a) required that all threshold transactions be recorded in SYCO;
- (b) required that Crown Melbourne report threshold transactions to AUSTRAC within 10 business days of the transaction taking place; and
- (c) provided guidance on what constituted a threshold transaction and the information required to be included in a TTR.

International Funds Transfer Instructions (IFTIs)

265 Between 1 March 2016 and 1 November 2020, the Crown Melbourne Standard Program:

- (a) required Crown Melbourne to report IFTIs in accordance with section 45 of the AML/CTF Act;
- (b) required staff to complete training on IFTI obligations under the AML/CTF Act and AML/CTF Rules, at least once every two years;
- (c) provided that the submission of IFTI reports was to be undertaken by credit control, with the responsibility for completion within the reporting times being with the Credit Control Manager;
- (d) required that random audits be conducted on IFTIs to ensure the accuracy and efficacy of IFTI reporting; and
- (e) included specific controls that required the reporting of IFTIs in relation to specific scenarios associated with the designated services provided by Crown Melbourne.

266 Between 1 March 2016 and 1 November 2020, the Crown Melbourne Guidelines:

- (a) required Credit Control to report IFTIs to AUSTRAC within 10 business days after the day on which the instruction was sent or received by the person, via AUSTRAC's online reporting system; and
- (b) provided guidance on the details to be reported to AUSTRAC, and the types of instructions requiring IFTIs.

F.8.2 Crown Perth

Suspicious Matter Reporting (SMRs)

267 Between 1 March 2016 and 1 November 2020, the Crown Perth Standard Program:

- (a) required Crown Perth to report suspicious matters in accordance with section 41 of the AML/CTF Act;
- (b) required staff to complete an AML/CTF online training module, at least once every two years;
- (c) provided a dedicated officer that was responsible for the management and continuous improvement of Crown Perth's AML/CTF obligations, including monitoring of gaming activity for the identification and reporting of suspicious matters to AUSTRAC; and

- (d) included a number of specific controls that required the reporting of suspicious activities with respect to specific scenarios arising from the designated services provided by Crown Perth.

268 Between 1 March 2016 and 1 November 2020, the Crown Perth AML SOPs:

- (a) required that all SMRs be reported to AUSTRAC within 3 business days after the day on which the suspicion formed unless in the case of terrorism financing where the report was to be lodged within 24 hours of the suspicion forming;
- (b) required the Legal Officer – AML to review reports from the SYCO daily alerts and i-Trak for all SMRs and report to AUSTRAC as required;
- (c) required that the AML/CTF Compliance Officer and the Legal Officer – AML meet and discuss suspicious matter reporting on a fortnightly basis; and
- (d) contained a monthly checklist to ensure Legal Services AML had complied with its relevant reporting obligations.

Threshold Transaction Reporting (TTRs)

269 Between 1 March 2016 and 1 November 2020, the Crown Perth Standard Program:

- (a) required Crown Perth to report threshold transactions in accordance with section 43 of the AML/CTF Act;
- (b) required staff to complete training on TTR obligations under the AML/CTF Act and AML/CTF Rules, at least once every two years; and
- (c) included a number of specific controls that required the reporting of threshold transactions in relation to specific scenarios associated with the designated services provided by Crown Perth.

270 Between 1 March 2016 and 1 November 2020, the Crown Perth AML SOPs:

- (a) required that Crown Perth report threshold transactions within 10 business days of the transaction taking place;
- (b) required the Legal Officer – AML to review reports from i-Trak for all TTRs and provide reports to AUSTRAC as required;
- (c) required the Legal Officer – AML to ensure all TTR forms for table buy ins and Table Games had been completed correctly and enter the details in SYCO where necessary;
- (d) required the Legal Officer – AML to review the cash transaction report submitted by the Cage each business day prior to uploading the report via the AUSTRAC online website;
- (e) required that the AML/CTF Compliance Officer and the Legal Officer – AML meet and discuss suspicious matter and threshold reporting on a fortnightly basis;
- (f) required that all buy ins be investigated to ensure that TTRs were completed and lodged if required; and
- (g) contained a monthly checklist to ensure Legal Services AML had complied with its relevant reporting obligations.

International Funds Transfer Instructions (IFTIs)

271 Between 1 March 2016 and 1 November 2020, the Crown Perth Standard Program:

- (a) required Crown Perth to report IFTIs in accordance with section 45 of the AML/CTF Act;
- (b) required staff to complete training in relation to IFTI obligations under the AML/CTF Act and AML/CTF Rules, at least once every two years;
- (c) provided that the submission of IFTI reports was a manual process, with the responsibility for lodgement within the reporting times being with the Legal Officer – AML or designee; and
- (d) included specific controls that required the reporting of IFTIs in relation to specific scenarios associated with the designated services provided by Crown Perth.

272 Between 1 March 2016 and 1 November 2020, the Crown Perth AML SOPs:

- (a) required the Legal Officer – AML to report IFTIs to AUSTRAC, within 10 business days after the day on which the instruction was sent or received by the person, via AUSTRAC's online reporting system;
- (b) provided that the telegraphic listing report be printed weekly and IFTIs listed on report be reported to AUSTRAC; and
- (c) contained a monthly checklist to ensure Legal Services AML had complied with its relevant reporting obligations.

F.8.3 Compliance with reporting obligations

273 Between 1 March 2016 and 1 November 2020, the Standard Part A Programs did not fully comply with the requirements of sub-paragraph 8.9.1(2) of the AML/CTF Rules and section 84(2)(c) in that the Part A systems and controls relating to the obligation to report under sections 41, 43 and 45 of the AML/CTF Act (**reporting obligations**):

- (a) did not include adequate guidance in relation to the reporting obligations;
- (b) did not include adequate assurance processes regarding Crown's reporting obligations;
- (c) with respect to SMR reporting obligations under section 41 of the AML/CTF Act:
 - (i) escalation processes with respect to unusual or suspicious matters were inadequate;
 - (ii) resourcing of the systems and controls for SMR reporting were inadequate, and were therefore incapable (as a matter of system or control design) of operating as intended; and
 - (iii) dispersed data sources for customer information limited Crown Melbourne's and Crown Perth's ability to understand a customer's transactional activity and to determine whether any particular activity was unusual; and
- (d) with respect to TTR obligations under section 43 of the AML/CTF Act:
 - (i) Crown Melbourne did not make and keep complete records of all designated services involving cash, and therefore did not have appropriate systems in place to identify and report all threshold transactions. For example, prior to April 2018, Suncity staff members would dispense Crown gaming chips in exchange for cash to junket players. In addition, junket players could exchange Crown chips for cash at the Suncity cash administration desk. Crown Melbourne made no record of cash transactions conducted in the private gaming rooms made available to the Suncity junket, including through the Suncity cash administration desk.

- (e) SMRs, TTRs and IFTIs relating to transactions on junket programs at Crown Melbourne and Crown Perth were often reported under the junket operator's name (with the junket representative as agent) rather than under the name of the junket player who conducted the transaction. This made it difficult for AUSTRAC and its law enforcement partners to understand the role of different parties to the suspicious activity or the transaction, including what transactions took place, the source of the funds, who instructed the movement of funds, the recipient of the funds and further details of the transaction.

F.9 Applicable Customer Identification Procedures (ACIPs)

- 274 At all times during the Relevant Period, Crown Melbourne and Crown Perth were required to have an AML/CTF program with a Part B that complied with the requirements described in Section D above.

F.9.1 Standard Part B Programs

- 275 Between 1 March 2016 and 1 November 2020, the Crown Melbourne Standard Part B Program was set out in clauses 20 to 24 and Annexures I and K of the Crown Melbourne Standard Program, and the Crown Perth Standard Part B Program was set out in clauses 18 to 20 and Appendices F and G of the Crown Perth Standard Program (together, the **Standard Part B Programs**). Relevantly:
- (a) clause 20 in each version of the Crown Melbourne Standard Part B Program, and clause 18 in each version of the Crown Perth Standard Part B Program, set out the circumstances in which a customer had to be identified;
 - (b) clauses 20, 23 and 24 and Annexures I and K in each version of the Crown Melbourne Standard Part B Program, and clause 18 and Appendices F and G in each version of the Crown Perth Standard Part B Program, set out the identification requirements for individual and non-individual (corporate) customers, and their beneficial owners, including the information that needed to be collected and verified;
 - (c) clause 21 in each version of the Crown Melbourne Standard Part B Program, and clause 19 in each version of the Crown Perth Standard Part B Program, set out the procedure that applied when verifying or re-verifying the identity of a high risk customer;
 - (d) clause 22 in each version of the Crown Melbourne Standard Part B Program, and clause 20 in each version of the Crown Perth Standard Part B Program, set out the procedure that applied when a Crown staff member suspected, on reasonable grounds, that a customer was not who they claimed to be;
 - (e) Annexures I and K in each version of the Crown Melbourne Standard Part B Program, clause 20 in version 8 of the Crown Melbourne Standard Part B Program, and clause 18 and Appendix F in each version of the Crown Perth Standard Part B Program, set out Crown's processes for resolving discrepancies that arose in the course of verifying KYC information collected about a customer; and
 - (f) Annexure I in each version of the Crown Melbourne Standard Part B Program, and Appendix F in each version of the Crown Perth Standard Part B Program, set out additional identification requirements for junket players.
- 276 In addition, between 1 March 2016 and 1 November 2020:
- (a) clause 14 in each version of the Crown Melbourne and Crown Perth Standard Part A Programs, clause 20 in version 8 of the Crown Melbourne Standard Part B Program, and

- clause 18 in versions 16 and 17 of the Crown Perth Standard Part B Program, set out trigger-based requirements for collecting additional KYC information about a customer;
- (b) clause 17 in each version of the Crown Melbourne Standard Part A Program set out requirements for PEPs, and clause 15 in each version of the Crown Perth Standard Part A Program and clause 18 in versions 16 and 17 of the Crown Perth Standard Part B Program, set out additional requirements for certain PEPs; and
- (c) the AUSTRAC Guidelines for Crown Melbourne and the Crown Perth AML SOPs for Crown Perth provided guidance relating to the identification procedures in the Standard Part B Programs.

F.9.2 Compliance of Standard Part B Programs

- 277 Between 1 March 2016 and 1 November 2020, the Standard Part B Programs did not fully comply with the requirements in Chapter 4 of the AML/CTF Rules, as described in paragraphs 278 to 291 below. As a result, between 1 March 2016 and 1 November 2020, the Standard Part B Programs did not comply with section 84(3)(b) of the AML/CTF Act.

Consideration of ML/TF risk factors

- 278 The Standard Part B Programs were required to include appropriate risk-based systems and controls to identify customers, as described in paragraph 80 above. In designing the risk-based systems and controls, each of Crown Melbourne and Crown Perth were required to have regard to the following risk factors in paragraph 4.1.3 of the AML/CTF Rules:
- (a) its customer types, including beneficial owners of customers and any PEPs;
 - (b) its customers' source of wealth and source of funds;
 - (c) the nature and purpose of the business relationships with its customers including, as appropriate, the collection of information relevant to that consideration;
 - (d) the control structures of its non-individual customers;
 - (e) the types of designated services it provided;
 - (f) the methods by which it delivered the designated services; and
 - (g) the foreign jurisdictions with which it dealt.
- 279 As described in F.1 above, neither Crown Melbourne nor Crown Perth appropriately assessed the ML/TF risks associated with its provision of designated services, including the risks associated with Crown's customer types (see paragraph 98), the types of designated services provided (see paragraphs 96 and 97), the methods by which designated services were delivered (see paragraphs 99 to 101) and the foreign jurisdictions dealt with (see paragraph 102). In particular, the Standard Part B Programs did not include appropriate risk-based systems and controls to:
- (a) identify customers who were high risk at the time the ACIP was being carried out.
 - (b) consider the nature and purpose of the business relationship with customers who were junket operators, junket representatives and junket players; and
 - (c) consider the risks posed by designated services under items 6, 7, 31 and 32, table 1, section 6 of the AML/CTF Act.
- 280 As a result:

- (a) the systems and controls in the Standard Part B Programs were not able to, and did not, appropriately consider the ML/TF risks associated with each of the risk factors in paragraph 4.1.3 of the AML/CTF Rules; and
- (b) the Part B Programs applied the same 'safe-harbour' ACIPs to all customers regardless of risk.

Additional KYC information

- 281 Paragraphs 4.2.5 and 4.2.8 of the AML/CTF Rules required that the Standard Part B Programs include appropriate risk-based systems and controls for determining whether, in addition to the Minimum KYC Information that must be collected and verified about a customer, any other KYC information be collected and verified about a customer.
- 282 The Standard Programs had trigger-based procedures for collecting additional KYC information. However, those procedures:
- (a) were not triggered at the time the ACIP was conducted and some did not form part of the Standard Part B Programs;
 - (b) did not include appropriate guidance for determining what additional KYC information should be collected;
 - (c) did not include appropriate risk-based systems and controls for determining whether, in addition to the minimum KYC information that needed to be verified, any other KYC information collected about a customer should be verified; and
 - (d) were not capable of being triggered consistently because the Part B Programs did not include appropriate systems and controls to identify customers who were high risk at the time the ACIP was being carried out.
- 283 As a result, the Standard Part B Programs did not include appropriate risk-based systems and controls to comply with the requirements in paragraphs 4.2.5 and 4.2.8 of the AML/CTF Rules. For example, there were no risk-based procedures in the Standard Part B Programs to determine whether to collect or verify additional KYC information relating to the beneficial ownership of funds used by the customer with respect to designated services or the beneficiaries of transactions being facilitated by the reporting entity on behalf of the customer including the destination of funds.

Agents of a customer

- 284 Paragraphs 4.11.2 to 4.11.4 of the AML/CTF Rules required that the Standard Part B Programs include:
- (a) appropriate procedures to collect information and documents about an agent of a customer who was an individual; and
 - (b) appropriate risk-based systems and controls for determining whether (and to what extent) Crown should verify the identity of an agent of a customer who was an individual.
- 285 The Standard Part B Programs did not include appropriate procedures, systems and controls to comply with the requirements in paragraphs 4.11.2 to 4.11.4 of the AML/CTF Rules, in that they did not include procedures, systems and controls relating to the collection and verification of documents and information in circumstances where an agent (including a junket representative) was acting on behalf of a customer that was an individual.

PEPs

- 286 Paragraph 4.13.1 of the AML/CTF Rules required that the Standard Part B Programs include appropriate risk-management systems to determine whether a customer or beneficial owner was a PEP. The Crown Melbourne and Crown Perth Standard Programs provided that PEPs could be identified through screening (using an external service provider) or the knowledge of Crown staff. However, for the reasons identified in paragraph 108, the screening processes were inadequate. As a result, the Standard Part B Programs did not include appropriate risk-management systems to comply with the requirement in paragraph 4.13.1 of the AML/CTF Rules. Also, by no later than June 2018, the Chief Legal Officer of Crown Resorts, who was also the AMLCO for both Crown Melbourne and Crown Perth, was advised by the Group General Manager AML that source of funds checks were not being conducted on foreign PEPs, contrary to the requirements of paragraph 4.13 of the AML/CTF Rules.
- 287 Paragraph 4.13.3 of the AML/CTF Rules required that the Standard Part B Programs include appropriate risk-management systems to undertake the following steps in relation to foreign PEPs and high ML/TF risk domestic and international organisation PEPs:
- (a) in the case of a beneficial owner, comply with the identification requirements specified in paragraphs 4.2.3 to 4.2.9 of the AML/CTF Rules as if the PEP was the customer;
 - (b) obtain senior management approval before establishing or continuing a business relationship with the customer and before the provision, or continued provision, of a designated service to the customer;
 - (c) take reasonable measures to establish the PEP's source of wealth and source of funds; and
 - (d) comply with the obligations in Chapter 15 of the AML/CTF Rules.
- 288 Although the Standard Programs identified the steps that had to be undertaken when a PEP was identified, including obtaining senior management approval, establishing the PEP's source of wealth and source of funds, and undertaking ECDD, the Standard Part B Programs did not include appropriate risk-management systems to ensure that the steps in paragraph 4.13.3 of the AML/CTF Rules were appropriately undertaken in all circumstances.

ACIPs applied to all customers

- 289 Section 32 of the AML/CTF Act required that Crown carry out the ACIP in respect of a customer, before commencing to provide a designated service to the customer. This requirement was subject to a number of exemptions. In particular:
- (a) Part 10.1 of the AML/CTF Rules exempted each of Crown Melbourne and Crown Perth from completing ACIP in circumstances where it was providing a prescribed designated service in table 3, section 6 of the AML/CTF Act, and the designated service involved an amount less than \$10,000. Paragraph 10.1.5 of the AML/CTF Rules provided that this exemption did not apply if Crown Melbourne or Crown Perth determined that it had to obtain and verify any KYC information about a customer in accordance with its ECDD Program and customer identification program.
 - (b) Paragraph 14.4 of the AML/CTF Rules exempted Crown from completing ACIP in circumstances where it was providing the designated service in item 14, table 3, section 6 of the AML/CTF Act, and, among other things, the value of the currency was less than \$1,000 (Australian or the foreign equivalent) and the proceeds and/or funding source of

the service was in the form of physical currency. Paragraph 14.5 of the AML/CTF Rules provided that this exemption did not apply where Crown Melbourne or Crown Perth determined in accordance with its ECDD Program that it should obtain and verify any KYC information about a customer in accordance with its customer identification program.

- 290 Between 1 March 2016 and 1 November 2020, clause 20 in each version of the Crown Melbourne Standard Part B Program, and clause 18 in each version of the Crown Perth Standard Part B Program set out the circumstances where a customer was required to be identified. These clauses did not cover all the circumstances where a customer was required to be identified. For example, these clauses required Crown Melbourne and Crown Perth to identify a customer when there was an exchange of foreign currency for the equivalent of AUD\$1,000 or more. However, these clauses did not require Crown Melbourne and Crown Perth to identify a customer in circumstances where there was an exchange of foreign currency by way of foreign drafts or travellers' cheques below AUD\$1,000, noting that the exemption in paragraph 14.4 of the AML/CTF Rules (as described in sub-paragraph 289(b) above) applied to physical currency only.

Information system and customer PIDs

- 291 For the reasons described in paragraph 260 above, Crown's information management systems did not enable Crown to be reasonably satisfied, where the customer was an individual, that the customer was the individual they claimed to be.

F.10 Joint AML/CTF Program

- 292 On 2 November 2020, a Joint AML/CTF Program was approved for Crown Melbourne and Crown Perth. In May 2021, the Crown Resorts Board approved the Financial Crime Compliance & Change Program (the **FCCCP**). The FCCCP is a significant program of work to uplift and implement the procedures, systems and controls that Crown adopts and maintains through its Joint AML/CTF Program, described further in paragraphs 304 to 307. From November 2020, the Joint AML/CTF Program started to improve Crown's identification, mitigation and management of ML/TF risk, and the subsequent versions of the Joint AML/CTF Program adopted during and after the Relevant Period have each made further progressive enhancements.
- 293 However, as at 2 November 2020, the Joint AML/CTF Program was yet to be fully operationalised. This was because many of the underlying procedures, systems and controls were yet to be adopted and implemented. In many cases, it took significant time to design, implement and embed these underlying procedures, systems and controls. As a result, the non-compliance described in section F in relation to the Standard Part A and Part B AML/CTF Programs persisted with respect to the Joint Part A and Part B AML/CTF Programs between 2 November 2020 and 1 March 2022 in the respects set out at paragraphs 294 to 301 below. As a result, between 2 November 2020 and 1 March 2022 Crown did not adopt and maintain an AML/CTF Program that met the requirements of the AML/CTF Act and Rules, contrary to section 81 of the AML/CTF Act.

The Joint Part A AML/CTF Program

- 294 The foundation of an AML/CTF Program is a ML/TF risk assessment. A Joint Part A Program will not meet the requirements of sections 85(2)(a) and (c) of the AML/CTF Act if it is not based on a ML/TF risk assessment that addresses the matters in paragraphs 9.1.3 and 9.1.4 of the AML/CTF Rules and if its procedures, systems and controls are not aligned to the ML/TF risks as identified in the assessment (see paragraphs 77(a) and (b) and 88).

- 295 Prior to December 2021, when Crown completed an ML/TF enterprise wide risk assessment (**ML/TF EWRA**), the ML/TF risks of designated services had not been comprehensively assessed by Crown having regard to the matters set out in paragraphs 9.1.3 and 9.1.4 of the AML/CTF Rules and in accordance with an appropriate written ML/TF risk assessment methodology. Prior to December 2021, in the case of some designated services, no ML/TF risk assessment had been conducted at all.³⁵ Crown faced the same inherent ML/TF risks on and from November 2020 as those described at paragraph 189, with the exception of the ML/TF risks posed by junkets, the overseas deposit services and the Hotel Card channel (all of which were no longer provided on and from adoption of the Joint AML/CTF Program on 2 November 2020).
- 296 The ML/TF EWRA methodology required Crown to assess its inherent ML/TF risk and its residual³⁶ ML/TF risk by assessing the extent to which its controls mitigated inherent ML/TF risks. Under the methodology for the ML/TF EWRA, the assessment of Crown's mitigating controls involved assessing the "coverage" of the controls (ie, the extent to which Crown has some or all of the relevant controls within its business relevant to the particular risk) and their "effectiveness" (ie, the extent to which the controls in place have been assessed as effective in identifying, mitigating and managing ML/TF risk).
- 297 The ML/TF EWRA assessed the coverage of Crown's controls but did not assess the effectiveness of those controls because during the period of assessment (1 July 2020 to 30 June 2021), limited testing had been capable of being performed as a result of the scale of the change made to existing controls and the introduction of new controls during this period. As a result, the ML/TF EWRA rated residual risk the same as inherent risk, both being 'high'.
- 298 A Joint Part A Program will not meet the requirements of sections 85(2)(a) and (c) of the AML/CTF Act if it does not include appropriate risk-based systems and controls that are:
- (a) aligned to an assessment of the ML/TF risks reasonably faced by a reporting entity;
 - (b) capable (as a matter of system or control design) of identifying, mitigating and managing ML/TF risks reasonably faced by the reporting entity, as assessed; and
 - (c) designed to ensure designated services are provided in a way that is consistent with ML/TF risk appetite.
- (See paragraphs 15 to 17, 78 and 135 above).
- 299 The lack of control effectiveness testing in the ML/TF EWRA meant Crown could not be satisfied that the criteria in paragraph 298 above were satisfied.
- 300 Whilst Crown addressed a number of the control deficiencies identified at Section F.4.4 above between 2 November 2020 and 1 March 2022, the control coverage, in aggregate, was still insufficient during this period to meet the requirements of section 85 of the AML/CTF Act and Chapters 9 and 15 of the AML/CTF Rules because:
- (a) Processes and frameworks for oversight and governance appropriate to an organisation the nature, size and complexity of Crown were still in the process of being designed and implemented.³⁷

³⁵ See paragraph 143 with respect to Credit Facilities and CCFs and paragraph 176 with respect to Crown Patron account channels.

³⁶ Residual risk is the risk remaining after systems and controls have been applied to mitigate and manage inherent ML/TF risks.

³⁷ See paragraphs 391 to 396, 398(a) and 400(a).

- (i) The Crown Resorts Board had not yet comprehensively articulated and approved its ML/TF risk appetite, which limited its ability to ensure appropriate risk-based systems and controls³⁸ were in place and to monitor whether the business was operating within ML/TF risk appetite.
 - (ii) Accountabilities, roles and responsibilities for processes under the Joint Part A Program were still being mapped and implemented and were yet to be accepted by senior management.
 - (iii) ML/TF key performance indicators and enhanced operational metrics to monitor the management of ML/TF risk were in the process of being implemented and upgraded.
 - (iv) The Governance, Risk and Compliance Tool (**GRC**) was still being developed. The GRC is a tool to support end-to-end ML/TF risk management and identification, mitigation and management of ML/TF risks across the business.
- (b) Operational procedures and frameworks were still in the process of being designed or redesigned and implemented in relation to:³⁹
- (i) uplifted and enhanced risk assessments of designated services, customers, channels and jurisdiction;
 - (ii) enhancements to aspects of the governance framework for transaction monitoring, including with respect to ML/TF risk coverage and transaction monitoring detection strategy design, development, deployment and review;
 - (iii) enhanced ECDD processes, including periodic review;
 - (iv) the capture of additional customer risk data attributes such as occupation, place of birth and citizenship;
 - (v) enhancements to Crown's risk mitigation measures to address gaps in controls for higher risk customers; and
 - (vi) enhancements to controls to mitigate and manage the ML/TF risks of poker.
- (c) the design, testing and implementation of automated AML/CTF processes took time. In the intervening period, the largely manual processes were not appropriate for a business the nature, size and complexity of Crown. In particular:
- (i) until February 2021, automated transaction monitoring alerts were still in the process of being designed;
 - (ii) from February 2021 to March 2022, automated alerts were still being refined and tested to an appropriate standard;
 - (iii) until April 2021, appropriate systems and workflow tools to review transactions the subject of unusual activity reports were not yet in place, with a significant backlog of reports that took time to action and review; and
 - (iv) from April 2021 to March 2022, resources to appropriately manage the backlog were still being recruited;⁴⁰

³⁸ See paragraphs 15 to 17 for an explanation of appropriate risk-based procedures, systems and controls.

³⁹ See paragraphs 397 to 399.

⁴⁰ See paragraphs 398 to 400.

- (d) information systems necessary to support and maintain the transaction monitoring and ECDD programs (such as automated case management) were in the process of being designed and implemented;⁴¹ and
 - (e) assurance processes were minimal and were still being designed and implemented.⁴²
- 301 By reason of the matters set out at paragraphs 295 to 300 in the period 1 November 2020 to 1 March 2022, the Joint AML/CTF Program:
- (a) did not have the primary purpose of identifying, mitigating and managing ML/TF risks in accordance with the AML/CTF Act (section 85(2)(a)); and
 - (b) did not yet fully comply with the requirements of Parts 9 and 15 of the AML/CTF Rules made under section 85(2)(c) of the AML/CTF Act.

The Joint Part B Program

- 302 The Joint Part B Program approved and adopted on 1 November 2020, and a subsequent version approved and adopted on 10 August 2021, made a number of enhancements to the Standard Part B Programs. For example:
- (a) each version included a requirement to collect and/or verify further information beyond minimum information required under the 'safe harbour' regime where, among other things, a customer progressed through a Crown Rewards membership tier or applied for access to a premium gaming room; and
 - (b) the 10 August 2021 version acknowledged Crown only provides designated services to individuals.
- 303 While each version of the Joint Part B Program was an improvement on prior versions, contrary to the requirements of section 85(3)(b) and paragraph 4.1.3 of the AML/CTF Rules, from November 2020 to 1 March 2022, other than as described in paragraph 302(a), neither version specified the customer types in respect of whom additional KYC information was required to be collected or collected and verified beyond the minimum information required under the 'safe harbour' regime (because the customer type is not low or medium risk at the time ACIP was being carried out).

The Financial Crime Compliance and Change Program (FCCCP)

- 304 Crown is committed to being an international leader in the casino sector in relation to ML/TF risk management and financial crime compliance. Its program of work to make good on this commitment is, and must necessarily always be, ongoing.
- 305 As noted in paragraph 292, from November 2020, AUSTRAC acknowledges that the Joint Part A procedures, systems and controls started to improve Crown's identification, mitigation and management of ML/TF risk, and the subsequent versions of the Joint AML/CTF Program adopted during and after the Relevant Period have each made further progressive enhancements.
- 306 Crown continues to engage constructively and transparently with AUSTRAC in relation to the FCCCP and the improvements it continues to make to its Joint AML/CTF Program. While the FCCCP is ongoing, the steps Crown has taken to date have significantly reduced its exposure to ML/TF risk.

⁴¹ See paragraph 400(a).

⁴² See paragraphs 403 and 398.

307 Crown has subjected the FCCCP and the Joint AML/CTF Program to external review. This includes the conduct of two independent reviews since the commencement of AUSTRAC's enforcement investigation, each conducted by an external risk consultant under Part 9.6 of the AML/CTF Rules. The report of the first review, completed on 31 March 2022, was shared with AUSTRAC. The report of the second review was finalised on 22 May 2023 and has been shared with AUSTRAC.

F.11 Conclusion

- 308 By reason of the matters at paragraphs 81 to 273, between 1 March 2016 and 1 November 2020, each of the Standard Part A Programs did not comply in material respects with the requirements of sections 84(2)(a) and 84(2)(c) of the AML/CTF Act and all the requirements of Chapters 8 and 15 of the AML/CTF Rules.
- 309 By reason of the matters admitted at paragraphs 274 to 291, from 1 March 2016 to 1 November 2020, each of the Standard Part B Programs did not comply in material respects with section 84(3)(b) of the AML/CTF Act and all the requirements of Chapter 4 of the AML/CTF Rules.
- 310 By reason of the matters at paragraphs 292 and 301, between 2 November 2020 and 1 March 2022 the Joint Part A Program did not comply in material respects with the requirements of sections 85(2)(a) and 85(2)(c) of the AML/CTF Act and all the requirements of Chapters 9 and 15 of the AML/CTF Rules.
- 311 By reason of the matters admitted at paragraphs 302 and 303, from November 2020 to 1 March 2022, each of the Joint Part B Programs did not comply in material respects with section 85(3)(b) of the AML/CTF Act and with all the requirements of Chapter 4 of the AML/CTF Rules
- 312 By reason of the matters admitted at paragraphs 308 to 311, during the Relevant Period, Crown commenced to provide designated services to customers without adopting and maintaining a compliant AML/CTF Program, contrary to section 81 of the AML/CTF Act.

G. CROWN'S CONTRAVENTIONS OF SECTION 36 OF THE AML/CTF ACT

- 313 At all times during the Relevant Period, Crown Melbourne and Crown Perth were required by section 36(1) of the AML/CTF Act to:
- (a) monitor their customers in relation to the provision of designated services at or through a permanent establishment of theirs in Australia, with a view to identifying, mitigating and managing the risk that Crown may reasonably face that the provision of a designated service at or through a permanent establishment of Crown in Australia might (whether inadvertently or otherwise) involve or facilitate money laundering; and
 - (b) do so in accordance with the AML/CTF Rules.
- 314 At all times during the Relevant Period, Crown Melbourne and Crown Perth were required by the AML/CTF Rules made under section 36(1), among other things:
- (a) to have regard to the nature, size and complexity of its business and the type of ML/TF risk it might reasonably face, including the risk posed by customer types;
 - (b) to include a TMP in their Part A programs that, among other things:
 - (i) includes appropriate risk-based systems and controls to monitor the transactions of customers;

- (ii) has the purpose of identifying, having regard to ML/TF risk (as defined in the AML/CTF Rules), any transaction that appears to be suspicious within the terms of s 41 of the AML/CTF Act; and
 - (iii) has regard to unusual patterns of transactions, which have no apparent economic or visible lawful purpose.
- (c) to include an ECDD program in their Part A programs that complies with the requirements of the AML/CTF Rules;
- (d) to apply the ECDD program when:
 - (i) Crown determined under its risk-based systems and controls that the ML/TF risk (as defined in the AML/CTF Rules) was high;
 - (ii) a designated service is being provided to a customer who is or who has a beneficial owner who is, a foreign PEP; or
 - (iii) a suspicion has arisen for the purposes of section 41 of the AML/CTF Act; and
- (e) to undertake the measures specified in rules 15.10(2) and 15.10(6) in the case of a customer who is a foreign PEP.

G.1 High risk customers

- 315 Each of the 60 customers set out in Appendix 1 was a customer of Crown Melbourne and/or Crown Perth on and from the date listed in column 2 (Crown Melbourne) or column 3 (Crown Perth) until the date listed in column 4 (Crown Melbourne) or column 5 (Crown Perth) (**High Risk Customers**).
- 316 At various times on and from 1 March 2016, Crown Melbourne and/or Crown Perth provided designated services within the meaning of tables 1 and 3, section 6 of the AML/CTF Act to each of the High Risk Customers.
- 317 High ML/TF risks were indicated in respect of each of the High Risk Customers:
- (a) 43 were junket operators, junket representatives or junket players.⁴³ The combined turnover for junkets associated with these 43 customers is \$69 billion. The turnover of the junkets of these High Risk Customers on and from 1 March 2016 ranged from around \$8 million (Customer 34) to approximately \$22.2 billion (Customer 1);⁴⁴
 - (b) 18 were foreign PEPs.⁴⁵ Of these, three customers were never identified as PEPs by either or both of Crown Melbourne or Crown Perth.⁴⁶ A further eight customers were identified by Crown Melbourne or Crown Perth as foreign PEPs several months or years after they became PEPs.⁴⁷ In addition, four customers were not consistently identified as PEPs across Crown Melbourne and Crown Perth.⁴⁸ In respect of one customer (Customer 44), Crown Melbourne identified the customer as a foreign PEP in 2017, but Crown Perth did not identify them as a foreign PEP until 2019;

⁴³ Customers 1-21, 23-29, 32-36, 42-46 and 48-52.

⁴⁴ For an explanation of turnover and its relationship to revenue and profit, see paragraphs 61 to 65.

⁴⁵ Customers 1, 3, 15, 17, 19, 21, 28, 29, 31, 32, 35, 43-46, 48, 49 and 52.

⁴⁶ Customers 1, 3, 15, 19, 21, 31 and 32.

⁴⁷ Customers 1, 3, 28, 29, 44, 45, 46 and 52.

⁴⁸ Customers 1, 3, 15, 44.

- (c) 40 were connected to other Crown Melbourne or Crown Perth customers in respect of whom Crown Melbourne or Crown Perth had formed suspicions and/or who had been banned from those properties;⁴⁹
- (d) 38 were involved (by receipt or transfer) in transactions of large sums totalling approximately \$450 million,⁵⁰ including:
 - (i) transfers of large values to or from other Crown Melbourne or Crown Perth customers in circumstances where Crown Melbourne or Crown Perth were not aware of, or did not understand, the connection between those customers. For example, Customer 39 transferred over \$4 million to other Crown customers, including Customer 40, between December 2017 and January 2019. Crown Melbourne did not fully appreciate the connection between Customer 39 and Customer 40 (who were operating a Ponzi scheme together) until it was served with a freezing order in July 2020; and
 - (ii) large financial transactions with unknown domestic or international third parties, including foreign remittance services. For example, between July 2016 and November 2017, Customer 15 received over \$5.5 million from third parties including corporate entities and international remittance services. Customer 38 was sent nearly \$7 million from an individual third party across 18 separate transactions;
- (e) seven customers transferred money – the value of which exceeded \$10.5 million – through overseas deposit services in circumstances where Crown Melbourne or Crown Perth did not conduct identification, source of funds or wealth checks.⁵¹ Customer 28 made several transfers in foreign currency to repay debts owed to Crown Aspinalls, including a cash deposit, via an agent, in the Suncity account, and a transfer from a third party to Crown Melbourne;⁵²
- (f) 18 customers who did not play on junkets turned over large amounts exceeding \$3 billion in total;⁵³
- (g) 31 engaged in transactions indicative of known ML/TF typologies and vulnerabilities including:⁵⁴
 - (i) 11 engaged in transactions indicative of structuring, the value of which exceeded \$1.2 million in total;⁵⁵
 - (ii) eight engaged in transactions indicative of cuckoo smurfing, the value of which exceeded \$17 million in total;⁵⁶
 - (iii) at least three⁵⁷ customers engaged in transactions indicative of offsetting, the value of which exceeded \$5 million in total, some of which were facilitated by Crown;

⁴⁹ Customers 1-3, 5-14, 16, 17, 20-29, 32, 33, 36, 38-41, 43-46, 49-51 and 54.

⁵⁰ Customers 1-6, 8, 9, 11-18, 18-22, 24-29, 34, 36-44, 49, 50 and 52.

⁵¹ Customers 2, 5, 16, 28, 29, 43 and 44.

⁵² Customers 26, 30, 31, 37-41, 47 and 53-60.

⁵³ For an explanation of turnover and its relationship to revenue and profit, see paragraphs 61 to 65.

⁵⁴ Customers 1-7, 9, 11, 15, 18-22, 26, 31-34, 36-38, 40, 43, 47 and 51-55.

⁵⁵ Customers 1-5, 26, 36, 43 and 53-55.

⁵⁶ Customers 4, 15, 21, 34, 36-38 and 43.

⁵⁷ Customers 1, 5 and 27.

- (iv) six customers engaged in transactions involving exchange of CVIs in amounts that were not commensurate with play, or where there was no evidence of play, the value of which exceeded \$2.5 million in total;⁵⁸
 - (v) 10 engaged in transactions indicative of quick turnover of funds, where deposits exceeded \$20 million in total and withdrawals exceeded \$39 million in total; and
 - (vi) 13 had parked funds in DABs or SKAs exceeding \$25 million in total.⁵⁹ Customer 7 has had over \$1.3 million lying dormant in his SKA since January 2016. Customer 47 had over \$200,000 parked in his SKA which, as at 30 April 2021, had been dormant for 505 days.
- (h) 27 engaged in large cash transactions totalling more than \$60.5 million.⁶⁰ For example, on 18 February 2018, Customer 14's junket representative withdrew \$2 million in cash from his account. In November 2017, Customer 5's junket representative presented approximately \$300,000 in cash to be deposited into Customer 5's DAB;
 - (i) 14 transacted with cash that appeared suspicious, including cash in plastic bags, shoeboxes or cardboard boxes, cash in rubber bands, small denominations of notes and counterfeit cash, in transactions totalling over \$10.5 million.⁶¹ For example, in February 2019, Customer 39 presented at the Cage with a shoe box full of cash totalling \$300,000 and comprising \$100 and \$50 notes. Two of the notes were found to be counterfeit;
 - (j) On and from 1 March 2016, Crown Melbourne and Crown Perth were aware of enquiries from law enforcement with respect to 14 High Risk Customers:⁶²
 - (i) in relation to four High Risk Customers, Crown was advised that at least one of the law enforcement requests related to money laundering or proceeds of crime investigations;⁶³ and
 - (ii) one customer was arrested at a Crown property;⁶⁴
 - (k) From 1 March 2016, Crown Melbourne and Crown Perth submitted approximately 1,026 SMRs in relation to the High Risk Customers. Of these, 210 related to Customer 1 and 234 related to Customer 2;
 - (l) Crown Melbourne and Crown Perth were aware that 18 customers had been suspected of, charged, arrested, prosecuted, convicted or imprisoned in connection with offences, including in some cases dealing with the proceeds of crime and money laundering.⁶⁵ For example, Crown Melbourne was aware that Customer 31 (who Crown Melbourne never rated as high risk) had previously been arrested in connection with bribery charges and was alleged to oversee the majority of prostitution, gambling, narcotics, extortion and smuggling in a foreign country. Two of these 18 customers were later acquitted of their charges;

⁵⁸ Customers 5, 26, 32, 40, 47 and 53.

⁵⁹ Customers 3, 4, 6, 7, 9, 18, 19, 21, 22, 36, 47, 51 and 52.

⁶⁰ Customers 1-3, 5, 14, 15, 20, 22-26, 33, 34, 36 and 38-40.

⁶¹ Customers 1-3, 5, 15, 20, 22, 23-25, 34, 39, 54 and 56.

⁶² Customers 1, 2, 4, 6, 18, 20, 23, 26, 29, 39, 48, 51, 56 and 60.

⁶³ Customers 20, 23, 26 and 56.

⁶⁴ Customer 56.

⁶⁵ Customers 2, 6, 23, 24, 26, 27, 30-32, 43, 51 and 56-60.

- (m) Crown Melbourne or Crown Perth accepted or transferred more than \$53 million of funds for, or on behalf of, 20 High Risk Customers through Crown Patron Accounts including the Riverbank or Southbank accounts, including deposits made by unknown third parties.⁶⁶ For example, Customer 39 received more than \$10 million from third parties via the Southbank account between February 2017 and February 2020. In August 2021, Crown Melbourne remitted \$1.5 million from Customer 50's DAB through a Crown Patron Account to an account Customer 50 held overseas;
- (n) Crown Melbourne allocated Customer 21 a pseudonym and a pseudonym PID. That customer turned over more than \$860 million under the pseudonym PID between June 2017 and September 2018.⁶⁷ Customer 21 was a foreign PEP and known, from at least March 2016, to be connected to Customer 2. In May 2016, Crown Melbourne made the Crown private jet available to Customer 21 under his pseudonym and pseudonym PID, although the charter of the private jet was paid for by Customer 21 and not Crown;
- (o) Crown Melbourne facilitated the transfer of funds by Customer 41 through the Hotel Card channel. By 11 March 2016, Customer 41 had transacted over \$3 million through Crown Towers Hotel for redemption at Crown Melbourne during FY16;
- (p) 23 High Risk Customers held CCFs with limits ranging from \$200,000 to \$140 million;⁶⁸ and
- (q) Crown Melbourne and Crown Perth failed to promptly obtain or appropriately consider information on the source of funds/wealth of High Risk Customers, in particular:
 - (i) In 2020 and 2021, four High Risk Customers refused, or ignored, requests from Crown Melbourne and/or Crown Perth to provide information regarding their source of funds/wealth.⁶⁹ Three of these customers turned over more than \$70 million from 1 March 2016;⁷⁰
 - (ii) In November 2020, one customer (Customer 53) completed a source of wealth declaration which identified his annual income to be less than \$250,000 and his profession to be a teacher (and that he was retired, working casually as at November 2020). The customer also identified additional income as \$500,000 to \$1,000,000 per annum, generated by share dividends. In 2022, Crown Melbourne reported this play to the AUSTRAC CEO as suspicious and inconsistent with Customer 53's reported wealth; and
 - (iii) Crown Melbourne and Crown Perth were aware of information suggesting that some customers were connected to organised crime or that their source of funds/wealth may otherwise not be legitimate but did not take appropriate risk-based measures in respect of those customers.

318 Crown Melbourne and/or Crown Perth should have recognised each High Risk Customer as high risk sooner than they did and, in some circumstances, failed to recognise the High Risk Customer as high risk at all. In particular:

⁶⁶ Customers 1-3, 5, 15, 16, 18, 21, 22, 34, 36-39, 41-44, 50 and 53.

⁶⁷ For an explanation of turnover and its relationship to revenue and profit, see paragraphs 61 to 65.

⁶⁸ Customers 1-6, 9, 11-13, 15-17, 19, 28, 29, 31, 34, 36, 37, 42, 51 and 52.

⁶⁹ Customers 34, 37, 54 and 55.

⁷⁰ For an explanation of turnover and its relationship to revenue and profit, see paragraphs 61 to 65.

- (a) 33 High Risk Customers were identified as high risk more than one year after they demonstrated high risk conduct;⁷¹
 - (b) 17 High Risk Customers were never identified as high risk by Crown Melbourne and/or Crown Perth by 1 March 2022;⁷²
 - (c) 3 High Risk Customers were identified as high risk by either Crown Melbourne or Crown Perth, but were not identified as high risk by the other reporting entity until at least a year later despite the customers' high risk conduct occurring at both properties; and⁷³
 - (d) in one case (Customer 44), Crown Melbourne rated the High Risk Customer as high risk until March 2019 and then reduced his risk rating to moderate, despite Customer 44 presenting high ML/TF risks.
- 319 At various points on and from 1 March 2016:
- (a) designated services provided to each High Risk Customer at Crown Melbourne and/or Crown Perth posed higher ML/TF risks;
 - (b) Crown Melbourne and/or Crown Perth did not undertake appropriate risk-based customer due diligence with respect to each High Risk Customer with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services; and
 - (c) Crown Melbourne and/or Crown Perth failed to undertake any risk-based customer due diligence with respect to six of the High Risk Customers.⁷⁴
- 320 At various points on and from 1 March 2016, Crown Melbourne and/or Crown Perth did not carry out appropriate risk-based ECDD measures with respect to each High Risk Customer in circumstances where:
- (a) Crown Melbourne and/or Crown Perth had formed a suspicion with respect to a High Risk Customer for the purposes of section 41 of the AML/CTF Act; or
 - (b) Crown Melbourne and/or Crown Perth had rated a High Risk Customer as high risk; or
 - (c) the High Risk Customer was a foreign PEP.
- 321 At various times on and from 1 March 2016, Crown Melbourne and/or Crown Perth senior management considered 43 High Risk Customers but, in the absence of appropriate guidance, failed to give adequate consideration to the ongoing ML/TF risks posed by these customers:⁷⁵
- (a) Senior management approved a continued business relationship or approved the continued provision of designated services to 28 of those customers on at least one occasion, despite the High Risk Customers having engaged in conduct indicating high ML/TF risks as set out at paragraph 317.⁷⁶ A number of these senior management decisions were based on customer or junket profiles prepared by the credit control team which did not adequately consider the ML/TF risks posed by the customers;
 - (b) WOLs issued to at least three High Risk Customers were revoked, despite the customers presenting ongoing high ML/TF risks.⁷⁷ For example, in late 2017, senior management

⁷¹ Customers 1-15, 20, 22, 23, 26, 28, 29, 31, 34, 39, 40, 46, 47, 51, 52, 55 and 58.

⁷² Customers 15, 16, 17, 18, 19, 21, 25, 31, 33, 36, 37, 38, 42, 45, 47, 50 and 53.

⁷³ Customers 3, 26 and 29.

⁷⁴ Customers 10, 12, 13, 20, 30 and 56.

⁷⁵ Customers 1-9, 11-22, 24, 26-29, 32, 34-36, 38-39, 43-45, 47-48, 50-54 and 59.

⁷⁶ Customers 1-8, 11, 14 – 21, 27 – 29, 32, 38, 44, 45, 50, 52, 54 and 59.

⁷⁷ Customers 27, 32 and 47.

made the decision to revoke Customer 32's WOL despite being aware of allegations that he was connected to a foreign political leader who had been convicted of war crimes, and to the CEO of a company used by that leader to smuggle weapons and fund war crimes. Customer 47 was issued with a WOL on three occasions on and from 1 March 2016, each of which was in place for a period of months. During the times when the WOL was lifted, Customer 47 engaged in transactions that were indicative of ML/TF typologies.

- 322 In January 2021, 16 of the High Risk Customers considered by senior management were subject to a review by the Crown Resorts POI Committee.⁷⁸ Fourteen of those customers had come to the Committee's attention through the NSW Independent Liquor & Gaming Authority inquiry.⁷⁹ At that meeting, 13 High Risk Customers were issued with a WOL,⁸⁰ eight of whom had been previously considered by senior management on at least one occasion.⁸¹
- 323 At no time did Crown Melbourne and/or Crown Perth senior management give consideration to whether the high ML/TF risks posed by nine High Risk Customers were within Crown Melbourne and/or Crown Perth's ML/TF risk appetite.⁸²

G1.1 High Risk customer case studies

- 324 The following three case studies illustrate how some High Risk customers exhibited multiple of the high risk factors described in paragraph 317, and how Crown failed to carry out appropriate due diligence with respect to these customers.

G1.1.1 Customer 1 – Suncity junket operator

- 325 Customer 1 was a customer of Crown Melbourne and Crown Perth from 2010-2021. Customer 1 was a junket operator and known by Crown to be the likely ultimate beneficial owner of the Suncity junket. Customer 1 was issued with a WOL on 22 January 2021 and an NRL (being a Notice Revoking Licence, the term used by Crown Perth to refer to a WOL) on 29 January 2021. The last designated service provided to Customer 1 was on 20 June 2020 in Crown Melbourne and 23 March 2020 in Crown Perth. From March 2012, media articles available from open source searches reported that Customer 1 and his associates were allegedly linked to organised crime. From September 2014, publicly available news articles identified that Customer 1 was a member of a foreign parliamentary advisory body.
- 326 Between 2010 and February 2016, Crown Melbourne gave 99 SMRs to the AUSTRAC CEO with respect to Customer 1. Crown Melbourne was in possession of a due diligence report dated March 2014 identifying Customer 1 as a foreign PEP. By January 2017, senior management was provided with information alleging Customer 1 was a former organised crime member and associated with individuals linked to organised crime, a foreign PEP, and linked to the receipt of \$81 million stolen from a central bank.
- 327 Crown Melbourne and Crown Perth did not rate Customer 1 as high risk until June-July 2017.
- 328 During the period from 2014 to 2018, Crown received six enquiries from law enforcement in relation to Customer 1 and the Suncity junket. In July and August 2019, Crown was aware of media reports alleging Customer 1 was linked to organised crime, and money laundering through Australian casinos, and that he was banned from entering Australia.

⁷⁸ Customers 1-3, 6-9, 11-14, 20, 29, 32, 34 and 46.

⁷⁹ Customers 1-3, 7-9, 11-14, 20, 29, 32 and 46.

⁸⁰ Customers 1-3, 7-9, 11-14, 20, 29 and 46.

⁸¹ Customers 1-3, 7-9, 11 and 20.

⁸² Customers 10, 25, 31, 33, 37, 41-42, 49 and 55.

- 329 During the period from March 2016 to March 2020, Crown gave the AUSTRAC CEO 215 SMRs with respect to Customer 1. Customer 1's profile was drawn to the attention of senior management, and considered, on at least 11 occasions from January 2017, but Crown did not end its business relationship with Customer 1 until January 2021.
- 330 At no time between 1 March 2016 and June 2020 (the date of the last designated service provided to Customer 1) did Crown appropriately monitor Customer 1's transactions on a risk-basis. During the period 1 March 2016 to 1 March 2020, Customer 1 was, as described in paragraph 224(a), associated with turnover of at least \$22 billion⁸³ in circumstances of high ML/TF risk:
- (a) From 1 March 2016 to late 2020, at least 252 Suncity-branded junket programs were operated at Crown by Customer 1 and their junket representatives, of which there were around 70. Crown provided Customer 1 with a standing credit line with a limit of \$30 million to operate their junket programs, which was reapproved by Crown management on a monthly basis from April 2016, and increased to \$50 million from March 2019 to March 2020.
 - (b) Throughout the Relevant Period, transactions conducted by Customer 1 and his junket representatives were indicative of higher ML/TF risks. These transactions totalled at least \$53 million from at least 276 transactions and included: unusual transactions and patterns of transactions; third party deposits and transfers including complex and large transactions on Customer 1's DAB; large cross-border movement of funds including through a Southbank account; and transactions indicative of ML/TF typologies including quick turnover of funds (without betting), refining, parked funds and suspicious cash transactions including through the Suncity cash administration desk.
 - (c) By way of example, in June 2017, Crown Melbourne agreed to a proposal by an apparent agent of Suncity to process a transaction through the Suncity account to settle a debt of \$9.6 million owed to Crown Melbourne by Customer 27. The debt would be settled by payment of 50% of the debt amount. Customer 27 had been excluded from the casino eight years earlier as a result of criminal activity and concerns over source of wealth but his WOL was withdrawn in June 2017 after consideration by Crown Melbourne's POI Committee to facilitate the debt repayment transaction. In June 2017, Customer 27 arranged for the deposit of an amount equivalent to \$4.8 million in cash (in HKD) into the Suncity account. This amount was never transferred to Crown Melbourne. In April 2018, Crown Melbourne agreed to offset this amount in the Suncity account against "lucky money" Crown Melbourne owed to Customer 1. On 1 May 2018, Customer 1 executed an authority directing that the amount equivalent to \$4.8m be transferred to Customer 1's account with Suncity in satisfaction of the debt Crown Melbourne owed to Customer 1. Again, the offset transaction, did not involve any funds being transferred from the Suncity account in Macau to a Crown bank account.

G1.1.2 Customer 3 – Meg-Star junket operator

- 331 Customer 3 was a customer of Crown Melbourne and Crown Perth from 2014-2021, and was the operator and likely ultimate beneficial owner of the Meg-Star junket. While Customer 3 was issued with a WOL on 22 January 2021 and an NRL on 29 January 2021, the last designated service provided to them was on 23 March 2020 in Crown Melbourne and 30 April 2020 in

⁸³ For an explanation of turnover and its relationship to revenue and profit, see paragraphs 61 to 65.

Crown Perth. As at 19 January 2022, Customer 3 had a Crown Perth DAB balance of \$45,959. By 2014, Crown Melbourne was aware that the Meg-Star International Company Limited had received investment of about \$2.5 million from a known member of a crime syndicate, and that Customer 3 had formerly been a Suncity executive. By March 2016, Crown Melbourne had given five SMRs to the AUSTRAC CEO. Customer 3 was also a foreign PEP.

- 332 Crown Melbourne did not rate Customer 3 as higher risk until April 2017; Crown Perth did not do so until January 2021.
- 333 Between 30 October 2016 and 5 March 2020, Crown gave the AUSTRAC CEO 87 SMRs in respect of Customer 3 and the Meg-Star junket involving over \$15 million and HKD1 million of funds. In 2020, Crown conducted due diligence searches which identified that a number of Meg-Star's known associates had been charged or accused of crimes including embezzlement, bribery in a foreign country and organising prostitution.
- 334 Crown did not issue Customer 3 with a WOL/NRL until January 2021. Crown Melbourne and Crown Perth did not provide Customer 3 with any designated services after this date.
- 335 At no time between March 2016 and late 2020 (when junket operations were suspended) did Crown appropriately monitor Customer 3's transactions on a risk basis. During the period March 2016 to late 2020 Customer 3 was associated with designated services of over \$34 million and HKD 2 million in circumstances of higher ML/TF risks, in addition to turnover associated with his junket:⁸⁴
- (a) Between 13 April 2016 and 23 March 2020, Customer 3 operated 268 Meg-Star junket programs at Crown. The total turnover of Meg-Star junket programs from December 2014 to late 2020 was approximately \$10.7 billion.⁸⁵ Customer 3 was provided with significant amounts of credit upon request, up to limits of \$100 million from 2018 to 2020 which was reapproved on a regular basis. From April 2018 to March 2020, Crown Melbourne made a cash administration desk available to the Meg-Star junket in private gaming rooms. Meg-Star junket staff dispensed chips in exchange for cash to junket players, and players could deposit cash with the junket.
 - (b) Throughout the Relevant Period, transactions by Customer 3 and associates of the Meg-Star junket included: large transfers to and from third parties including transactions related to debts; large cross-border movements of funds including into the Southbank and Riverbank accounts; large amounts of cash and cash that appeared suspicious (including large volumes of cash bundled in clear plastic bags); and transactions indicative of ML/TF typologies including structuring, quick turnover of funds (without betting) and parked funds. Customer 26 was a junket representative for the Meg-Star junket. Crown records note that law enforcement enquiries were received in 2012 and 2014 in relation to Customer 26 and possible operation of illegal brothels and using Crown for money laundering. Crown did not become aware until mid-2019 that Customer 26 owned a brothel linked to money laundering in court proceedings in 2015, and which was the subject of tribunal proceedings in 2014 involving allegations of human sex trafficking. In August 2019, Crown Melbourne issued a WOL. In June 2020, Crown Perth issued an NRL. During the period from March 2016 to June 2020, Customer 26 was associated with turnover exceeding \$113 million,⁸⁶ including in connection with the Meg-Star junket.

⁸⁴ For an explanation of turnover and its relationship to revenue and profit, see paragraphs 61 to 65.

⁸⁵ For an explanation of turnover and its relationship to revenue and profit, see paragraphs 61 to 65.

⁸⁶ For an explanation of turnover and its relationship to revenue and profit, see paragraphs 61 to 65.

G.1.1.3 Customer 59 – domestic customer

- 336 Customer 59 was a customer of Crown Melbourne from March 2006 to February 2020. On 2 November 2016, Crown Melbourne performed a risk intelligence search on Customer 59, which reported that they had been charged with trafficking in methamphetamine and being sentenced to 19 months imprisonment in June 2014. During the period from 2015 to 2018, Crown Melbourne received 11 enquiries from law enforcement in respect of Customer 59.
- 337 On 14 November 2016, the POI Committee determined that it would continue to conduct a business relationship with Customer 59 despite the higher ML/TF risk that he posed. In 2017 and 2018, Customer 59's rate of play increased significantly. Between 2017 and 2019, they lost approximately \$990,000.
- 338 Between March 2017 and December 2018, Crown responded to multiple law enforcement requests for information in relation to suspected large-scale money laundering from proceeds of drug related activities. From July 2018, Crown Melbourne was aware that law enforcement was investigating Customer 59 in relation to suspected large-scale money laundering from proceeds of drug-related activities. On 7 November 2018 and 28 January 2020, Crown Melbourne conducted further risk intelligence and media searches on Customer 59, which reported on Customer 59's convictions for drugs trafficking, including further charges in March 2019.
- 339 At no time between 1 March 2016 and February 2020 did Crown Melbourne take appropriate steps to understand whether Customer 59's source of funds/wealth was legitimate, or whether his transactions had a lawful purpose. Crown Melbourne did not issue Customer 59 with a WOL until November 2020.
- 340 At no time between 1 March 2016 and February 2020 did Crown appropriately monitor Customer 59's transactions on a risk-basis. During the period March 2016 to November 2020 Customer 59 presented higher ML/TF risks, including that:
- (a) between 2016 and 2018, Customer 59 had received large machine payouts from EGMs totalling over \$1.3 million; and
 - (b) in 2018, Customer 59 had been paid \$56,423 in cancel credits, which is indicative of the ML/TF typology of quick turnover (without betting); by January 2020, Customer 59 had over \$1 million in losses. Customer 59 carried large amounts of cash, and received table 3 designated services in circumstances of escalating rates of high turnover. For example, Crown Melbourne recorded that Customer 59's annual turnover for 2016 was \$1,258,752; and his annual turnover for 2017 was \$2,940,498.⁸⁷

G.2 Typology customers

- 341 At various times between 1 March 2016 and 1 March 2022, Crown Melbourne or Crown Perth (as specified in column 3 of Appendix 2) provided a DAB and/or SKA to each of the customers listed in column 1 of Appendix 2 (**Typology Customers**).
- 342 At various points between 1 March 2016 and 1 March 2022, Crown Melbourne or Crown Perth provided the Typology Customers with designated services within the meaning of item 13, table 3, section 6 of the AML/CTF Act with respect to the DABs and SKAs referred to in paragraph 341 above.

⁸⁷ For an explanation of turnover and its relationship to revenue and profit, see paragraphs 61 to 65.

- (a) Crown Melbourne or Crown Perth accepted or transferred funds for, or on behalf of, each of the Typology Customers through a Crown Patron Account.
 - (b) These funds were deposited into, or transferred from, DABs and/or SKAs provided to each Typology Customer.
 - (c) Transactions on DABs and SKAs were designated services provided by Crown Melbourne or Crown Perth to each customer within the meaning of item 13, table 3, section 6 of the AML/CTF Act.
- 343 At various points between 1 March 2016 and 1 March 2022, Crown Melbourne or Crown Perth did not apply appropriate risk-based transaction monitoring (see section E.6 above) to the DABs and SKAs of the Typology Customers to detect transactions potentially indicative of:
- (a) structuring;
 - (b) cuckoo smurfing;
 - (c) smurfing;
 - (d) chip or CVI cashing with minimal or no gaming activity; or
 - (e) quick turnover of chips or CVIs with minimal or no gaming activity.
- 344 As a consequence of this, Crown failed to identify transactions that were indicative of ML/TF typologies across the accounts. For example:
- (a) Between 2 February 2019 and 21 January 2020, one customer conducted a series of transactions that were indicative of structuring on 11 separate occasions. The customer made 41 deposits into his DAB totalling \$193,296. Another customer made 16 deposits under \$10,000 totalling \$75,100 between 27 October 2019 and 3 November 2019.
 - (b) On 13 July 2017, one customer deposited \$135,000 in cash into the Southbank account over 18 transactions, each of which were indicative of cuckoo smurfing. The following day, another customer deposited \$42,000 cash into the Riverbank account over five transactions, some of which took place in Sydney.
 - (c) Between January 2017 and July 2019, one customer engaged in 42 transactions that were indicative of quick turnover of CVIs with minimal gambling activity. Their transactions totalled over \$2.5 million in debits and over \$2 million in credits. Between March 2016 and February 2020, one customer engaged in 249 transactions that were indicative of quick turnover of funds with minimal gambling activity. Their transactions totalled over \$3 million in debits and over \$2 million in credits. Another customer engaged in 167 transactions indicative of quick turnover of funds with minimal gambling activity between June 2016 and June 2019, totalling over \$1.3 million in debits and \$1.1 million in credits (see Schedule 2, section F).
- 345 Certain transactions conducted on the DABs and SKAs by the Typology Customers at various points on and from 1 March 2016 had the indicia of one or more of the typologies referred to at paragraph 343 above.
- 346 By reason of the matters set out at paragraphs 341 to 345 above, at various points on and from 1 March 2016, Crown Melbourne or Crown Perth did not monitor each of the Typology Customers in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced, in accordance with the AML/CTF Rules.

G.3 Contraventions

347 By reason of the matters set out at paragraphs 315 to 346 above, on and from 1 March 2016:

- (a) Crown Melbourne contravened section 36(1) of the AML/CTF Act by failing to monitor 380 High Risk Customers and Typology Customers in relation to the provision of designated services:
 - (i) with a view to identifying, mitigating and managing the money laundering risks that Crown Melbourne reasonably faced; and
 - (ii) in accordance with Chapter 15 of the AML/CTF Rules; and
- (b) Crown Perth contravened section 36(1) of the AML/CTF Act by failing to monitor 166 High Risk Customers and Typology Customers in relation to the provision of designated services:
 - (i) with a view to identifying, mitigating and managing the money laundering risks that Crown Perth reasonably faced; and
 - (ii) in accordance with Chapter 15 of the AML/CTF Rules.

H. FACTS RELEVANT TO RELIEF

H.1 Nature and extent of the contraventions

H.1.1 Section 81 of the Act – AML/CTF Programs

348 Crown Melbourne and Crown Perth contravened section 81 of the AML/CTF Act from 1 March 2016 to 1 March 2022 by commencing to provide designated services in circumstances where their Part A Programs did not, for the reasons set out at paragraphs 308 to 312, fully comply with the requirements of the AML/CTF Act and Rules. Each time Crown Melbourne and Crown Perth commenced to provide a designated service during that period, they contravened section 81 of the AML/CTF Act. The contraventions are significant in number but too numerous to quantify. The maximum penalty for each contravention ranges from \$18 million to \$22.2 million.

H.1.1.1 Part A – Program failures with respect to the identification, mitigation and management of ML/TF risks

349 These contraventions were serious because:

- (a) The ML/TF risks of Crown's business were high. The vulnerability of the casino industry to ML/TF risks was well-known and the subject of typologies and guidance published by relevant authorities, including AUSTRAC.
- (b) The AML/CTF Act reposed a high degree of trust in Crown to identify, mitigate and manage the ML/TF risks of its own business.
- (c) Part A of an AML/CTF Program is the framework through which boards and senior management understand their ML/TF risks and determine their ML/TF risk appetite. It is the framework through which boards and senior management determine the risk-based controls they will apply to mitigate and manage the ML/TF risks they choose to accept.
- (d) The requirement to carry out and maintain current ML/TF risk assessments of designated services is central and foundational to the AML/CTF Program and to the AML/CTF Act.
- (e) Crown was required to assess the ML/TF risks of all designated services it provided – both gaming and financial.

- (f) Having failed to properly assess and understand its ML/TF risk across its business, Crown's Standard and Joint Part A Programs were incapable of appropriately mitigating and managing its high ML/TF risks.
- (g) In the absence of appropriate ML/TF risk management, a number of high-risk practices, channels and customer relationships evolved at Crown Melbourne and Crown Perth (such as the Southbank, Riverbank and Suncity accounts and the Hotel Card channel) which exacerbated the already high ML/TF risks of designated services.
- (h) Crown failed to appropriately identify, mitigate and manage the high ML/TF risks of junkets until it banned dealings with junkets in November 2020. The junket channel presented high ML/TF risks due to the large amounts of money involved which was often moved across borders. Junkets often lacked transparency and provided a level of anonymity to players and the sources of their funds. In the Relevant Period, Crown Melbourne generated \$1,365 million in revenue from junkets. Crown Perth's revenue from junket operations from 1 March 2016 was approximately \$320 million. Of the total junket revenue of approximately \$1,685 million across the Relevant Period, approximately \$1,109 million was attributable to the high risk customers referred to in paragraph 355(c) below.⁸⁸
- (i) The deficiencies with Crown's Part A Programs persisted for a number of years and were systemic, although the Joint Part A Programs progressively improved Crown's identification, mitigation and management of ML/TF risk. While the FCCCCP is ongoing, the steps Crown has taken to date have significantly reduced its exposure to ML/TF risk.
- (j) The Standard Part A Programs were not subject to appropriate assurance, review or oversight. In the period November 2020 to 1 March 2022, assurance processes and oversight frameworks were still being implemented.
- (k) The requirement in Part 8.6 of the AML/CTF Rules to conduct regular independent reviews of Part A of a standard AML/CTF program is intended to give boards and senior management assurance that AML/CTF risk management is compliant with the AML/CTF Act. The same requirement applies to Joint Part A Programs in Part 9.6 of the AML/CTF Rules. During the Relevant Period, neither Crown Melbourne nor Crown Perth completed an independent review that satisfied all of the requirements of paragraph 8.6.5 of the AML/CTF Rules, which set out the requirements for the purpose of the review. An independent review of Part A of the Joint AML/CTF Program in operation on and from 1 November 2020 was completed on 31 March 2022.
- (l) By no later than June 2018, the Chief Legal Officer of Crown Resorts, who was also the AMLCO for both Crown Melbourne and Crown Perth, was advised by the Group General Manager AML that the Crown Melbourne AML/CTF Program had not been updated for some time and that key ML/TF risks were not on the Risk Register and did not form part of the TMP.
- (m) In the absence of appropriate risk-based controls in Crown's Part A Programs, money could be moved into and out of the casinos, and within the casinos, in ways that lacked transparency as to the source and ownership of funds. This made Crown Melbourne and Crown Perth vulnerable to the risk of criminal exploitation. Crown's management of these risks started to improve from November 2020.

⁸⁸ For an explanation of revenue see paragraphs 63 to 65.

- (n) Crown's failure to appropriately identify and manage the ML/TF risks of its business and to appropriately monitor these transactions for suspicious activity has resulted in the loss of opportunity to detect, trace and disrupt possible unlawful activity, including possible money laundering.

H.1.1.2 Part A – Transaction monitoring program (TMP)

350 These contraventions were serious because:

- (a) The AML/CTF Act reposed a high degree of trust in Crown to monitor transactions, having regard to the ML/TF risks of its own business.
- (b) Appropriate risk-based transaction monitoring is central to ensuring that matters that may be suspicious for the purposes of section 41 of the AML/CTF Act are identified and reported to AUSTRAC and law enforcement. Appropriate risk-based transaction monitoring is central to Crown's understanding of its own ML/TF risks, including emerging risks.
- (c) The deficiencies in Crown's TMP were systemic and persisted over a number of years.
 - (i) It was not aligned to an appropriate ML/TF risk assessment.
 - (ii) It did not appropriately cover all designated services provided by Crown – both financial and gaming.
 - (iii) It was not capable of detecting all well-known ML/TF typologies and vulnerabilities faced by casinos.
 - (iv) Transaction monitoring was predominantly manual and incapable of appropriately detecting unusual or suspicious transactions, given the nature, size and complexity of Crown's business.
 - (v) The TMPs were not capable of operating as intended, due to significant deficiencies in information management systems and in the resourcing of the AML/CTF compliance function.
- (d) Prior to November 2020, Crown did not appropriately monitor payment flows through Crown Patron Accounts, including international payment flows. Nor did Crown appropriately monitor transactions, including cross-border transactions through high risk junket channels. These failures exposed the Australian financial system and the Australian community to ML/TF risks. From November 2020, monitoring of credits and debits into DABs via Crown Patron Accounts started to improve, although this was predominantly manual.
- (e) During the Relevant Period, Crown's TMP was not subject to appropriate assurance, and an independent review was not completed until March 2022.
- (f) By no later than June 2018, the Chief Legal Officer of Crown Resorts, who was also the AMLCO for both Crown Melbourne and Crown Perth, was advised by the Group General Manager AML of multiple deficiencies that impact the TMP, including that:
 - (i) key ML/TF risks were not on the Risk Register and did not form part of the transaction monitoring program;
 - (ii) there was a decision not to directly monitor transactional activity on EGMs and ETGs, although unusual activity could be picked up if another trigger hit. The

Group General Manager AML recommended that this decision be taken to the Board for consideration as to its comfort level;

- (iii) there were no specific controls at Crown Melbourne to monitor for transactions under \$10,000 for certain risks, resulting in vulnerability to structuring;
 - (iv) there was a need to investigate automation of elements of the transaction monitoring program. Relevantly, work did not start on the project to build an automated transaction monitoring framework until 2019 and it did not go live until February 2021, at which point it continued to operate in parallel with Crown Melbourne's manual monitoring system; and
 - (v) the existence of multiple accounts for customers was impacting transaction monitoring, complicated disclosures to law enforcement agencies and required multiple data points to be checked to ensure that information on SMRs was correct.
- (g) Crown's failure to appropriately monitor billions of dollars in transactions (including international payment flows) impacted its ability to identify and disrupt possible suspicious activity, and to report suspicious matters to AUSTRAC and law enforcement.⁸⁹

H.1.1.3 Part A – ECDD Program

351 These contraventions were serious because:

- (a) Crown regularly dealt with high risk customers, including junket customers, international VIP customers, high rollers and foreign PEPs. The high ML/TF risks posed by these customer types were well-known and the subject of typologies and guidance published by relevant authorities including AUSTRAC.
- (b) During the Relevant Period, the ECDD Programs were not capable of identifying and escalating all customers who were required by the AML/CTF Act and Rules to be subject to enhanced due diligence due to their high risks.
- (c) Nor, during the Relevant Period, did the ECDD Programs include adequate guidance on the ECDD measures to be applied when a customer was identified and escalated.
- (d) In particular, during the Relevant Period, the ECDD Programs did not include appropriate systems and controls to obtain, analyse and record source of wealth and source of funds information with respect to customers. This, in turn, created a risk of inhibiting the ability of law enforcement and AUSTRAC to trace money to its source, and associated law enforcement investigations, prosecutions and the recovery of proceeds of crimes.
- (e) The ECDD Programs were not supported by appropriate information management and record keeping. As well as being dispersed across multiple IT systems, customer records were also dispersed across multiple customer IDs and names, including, in a small number of cases, pseudonyms which Crown assigned to certain customers. Crown Melbourne's and Crown Perth's IT and record keeping systems were not capable of providing a complete view of customers' transactions and ML/TF risk profiles for ECDD purposes.
- (f) During the Relevant Period, the ECDD Programs did not include appropriate systems and controls to ensure that customers were escalated to senior management for approval

⁸⁹ For an explanation of turnover and its relationship to revenue and profit, see paragraphs 61 to 65.

when required, and to assist senior management with determining whether Crown should continue a business relationship with a customer, or continue to provide a designated service to a customer.

- (g) The deficiencies in the ECDD Programs meant that Crown was limited in its ability to appropriately detect and manage customers whose transactional activity was highly indicative of ML/TF risks and typologies. It also meant that Crown continued to deal with certain high risk customers without adequate consideration as to whether an ongoing relationship was appropriate, having regard to ML/TF risks. These failures exposed Crown Melbourne and Crown Perth to the risk of being exploited by organised crime.
- (h) By no later than June 2018, the Chief Legal Officer of Crown Resorts, who was also the AMLCO for both Crown Melbourne and Crown Perth, was advised by the Group General Manager AML of multiple deficiencies relating to ECDD, including that:
 - (i) the assessment and analysis of customer risk by Crown Melbourne was arbitrary and not subject to any concrete risk parameters;
 - (ii) Crown's ECDD processes should be updated to make it clearer as to when source of funds information would be sought and what specified source of wealth or source of funds checks would be conducted, particularly with respect to third party transfers; and
 - (iii) the issue of source of wealth/funds under the AML/CTF Programs should be taken to the Board for its consideration as to its comfort level.

H.1.1.4 Part A- Systems and controls for SMR, TTR and IFTI reporting

352 These contraventions were serious because:

- (a) As a result of the failure to include appropriate systems and controls in the Standard Part A Programs to ensure compliance with the obligation to report under sections 41, 43 and 45 of the AML/CTF Act, AUSTRAC and law enforcement agencies were denied financial intelligence to which they were entitled. This undermines the objectives of the AML/CTF Act and impacts the ability of AUSTRAC and law enforcement to carry out their functions. In particular, failure to provide required reports or required information to AUSTRAC inhibits law enforcement investigations, prosecutions and the recovery of proceeds of crime.
- (b) By no later than June 2018, the Chief Legal Officer of Crown Resorts, who was also the AMLCO for both Crown Melbourne and Crown Perth, was advised by the Group General Manager AML that the CTRM (Melbourne) essentially acted as a post box on unusual activity report (**UAR**) forms submitted by frontline staff, supplementing them where relevant but otherwise just passing them on, and was advised that resourcing in the AML team in both Melbourne and Perth was stretched to the limit.
- (c) On or about September 2020, Crown Melbourne and Crown Perth commenced a number of transaction monitoring lookbacks over designated services provided to customers from 1994. As a result of these transaction monitoring lookbacks and other customer-related lookback reviews, Crown Melbourne and Crown Perth have formed suspicions resulting in over 400 SMRs being given to the AUSTRAC CEO to date.

H.1.1.5 Part B - ACIP

353 These contraventions were serious because:

- (a) Crown regularly dealt with high risk customers, including junket customers, international VIP customers, high rollers and foreign PEPs. The high ML/TF risks posed by these customer types were well-known and the subject of typologies and guidance published by relevant authorities including AUSTRAC.
- (b) It was not appropriate for Crown to apply low risk 'safe harbour' ACIP to all of its customers by default. Additional KYC information should have been collected and verified for high risk customer types. In determining, on a risk-basis, what additional KYC information should have been collected and verified, Crown should have considered the ML/TF risks of the table 1, section 6 designated services it was providing.
- (c) The failure to obtain appropriate source of wealth/funds information at the time of the ACIP, where required on a risk-basis, affected the operation of processes in Crown's Part A Programs. For example, this failure impacted Crown Melbourne's and Crown Perth's ability to identify unusual or suspicious transactions, such as unusually high turnover or losses.
- (d) The failure to obtain appropriate source of wealth/funds information at the time of the ACIP, where required on a risk-basis, also impacted Crown's ability to mitigate and manage the ML/TF risks of foreign PEPs. By no later than June 2018, the Chief Legal Officer of Crown Resorts, who was also the AMLCO for both Crown Melbourne and Crown Perth, was advised by the Group General Manager AML that source of funds checks were not being conducted on foreign PEPs, contrary to requirements of rule 4.13.
- (e) Further, Crown's failure to include appropriate procedures, systems and controls relating to the collection and verification of documents and information relating to agents of customers (including junket representatives) impacted its ability to appropriately mitigate and manage the ML/TF risks of certain high risk customers and understand the ML/TF risks of third-party transactions.
- (f) The complexity and volume of designated services provided to customers, combined with the absence of appropriate KYC information (particularly source of funds and source of wealth information), significantly limited Crown Melbourne's and Crown Perth's ability to fully understand who they were dealing with as a customer.
- (g) The deficiencies with Crown's Part B Programs persisted for a number of years and were systemic. During the Relevant Period, the Part B Programs were not subject to appropriate assurance or review, and prior to 2 November 2020, oversight.
- (h) The deficiencies in Crown Melbourne's and Crown Perth's information management systems limited their ability to know who their customers were, as at the time the ACIP was carried out.
- (i) Deficiencies in KYC records inhibit the ability of law enforcement and AUSTRAC to trace money to its source. This, in turn, can inhibit law enforcement investigations, prosecutions and the recovery of proceeds of crimes.

H.1.2 Section 36 of the Act – Ongoing customer due diligence

- 354 Crown Melbourne and Crown Perth contravened section 36 of the AML/CTF Act between 1 March 2016 and 1 March 2022.
- 355 These contraventions were serious because:

- (a) Crown regularly dealt with high risk customers, including junket customers, international VIP customers, high rollers and foreign PEPs. The high ML/TF risks posed by these customer types were well-known and the subject of typologies and guidance published by relevant authorities including AUSTRAC.
- (b) Crown's failure to conduct appropriate OCDD in relation to 505 customers (who were either high risk or were transacting in ways that involved high risks) was systemic and occurred over a number of years. This failure exposed Crown and the Australian community to risks of serious organised crime.
- (c) 60 of these 505 customers were high risk customers and had turnover in excess of \$70 billion and revenue to Crown of about \$1,246 million.⁹⁰ Crown Melbourne and Crown Perth continued their business relationships with these high value customers, some of whom had reported links to organised crime, in the absence of appropriate due diligence.
- (d) 445 of these 505 customers engaged in transactions that were indicative of money laundering on the Crown Patron Accounts. Crown Melbourne and Crown Perth failed to conduct appropriate risk-based due diligence in respect of these customers.
- (e) Had Crown appropriately monitored its customers, it may have identified activity indicative of ML/TF typologies sooner. Had this activity been identified sooner, it could have been investigated and, where determined to be suspicious, reported to AUSTRAC and law enforcement sooner, through SMRs. Had suspicious activity been identified sooner, Crown would have been in a position to undertake additional steps to identify, mitigate and manage the ongoing risks.
- (f) Crown was aware of reports that 17 High Risk Customers were charged with, convicted of, or implicated in serious offences either prior to or after receiving designated services. One individual was reported to have been charged in relation to activity that took place at Crown Melbourne.⁹¹

H.2 Loss or damage suffered

- 356 Crown Melbourne and Crown Perth operate in an industry known, internationally and within Australia, to pose high ML/TF risks. As a result of the contraventions admitted in Sections F and G above, the casinos facilitated the provision of designated services with turnover in the billions of dollars in the absence of appropriate AML/CTF controls.⁹²
- 357 Crown Melbourne and Crown Perth facilitated the movement of money into and out of the casino environment through their bank accounts by way of designated remittance services. By facilitating this movement of money without appropriate AML/CTF controls, Crown Melbourne and Crown Perth exposed their banking partners and other financial institutions in transaction chains to ML/TF risks.
- 358 As a result of Crown Melbourne's and Crown Perth's non-compliance, the Australian and global community and financial system has been exposed to systemic ML/TF risks over many years. It is likely that many ML/TF risks were realised and that Crown Melbourne and Crown Perth were at risk of being exploited by organised crime.

⁹⁰ For an explanation of turnover and its relationship to revenue and profit, see paragraphs 61 to 65.

⁹¹ Customer 30.

⁹² For an explanation of turnover and its relationship to revenue and profit, see paragraphs 61 to 65.

- 359 Appropriate risk-based controls were not in place to enable Crown Melbourne or Crown Perth to understand the sources of money moving through these high-risk channels, or whether there was a risk that money was illicit. These business practices and risk management failures exposed Crown Melbourne and Crown Perth to the risk of money laundering.
- 360 In the absence of appropriate ML/TF controls, Crown Melbourne and Crown Perth facilitated the movement of significant amounts of money through high risk and non-transparent channels. A significant number of these transactions were also indicative of ML/TF typologies or vulnerabilities. By way of example:
- (a) An external auditor's report concluded that the value of deposits into the Southbank and Riverbank accounts between 2013 and 2019, with features indicative of money laundering, was over \$290 million. In addition, an external auditor's report identified transactions totalling over \$28 million through the Crown Patron Accounts containing money laundering indicia between 2020 and April 2021.
 - (b) About \$50 million was deposited through the Hotel Card channel by Crown Melbourne from 1 March 2016 to October 2016.
 - (c) In May 2018, Crown Melbourne remitted \$4.8 million through the Suncity account deposit service channel to settle a \$9.6 million debt owed to Crown by a former customer, who had been excluded from the casino eight years earlier as a result of criminal activity and concerns over source of wealth.
 - (d) From 1 March 2016 to December 2018, there were at least 75 suspicious 'incidents' involving cash in a private gaming room in Crown Melbourne to which one junket operator was given exclusive access. Cash transactions totalling approximately \$23 million were involved, in circumstances where the identity of some of the persons presenting and removing the cash from the casino premises was and remains unknown.
 - (e) Crown Melbourne and Crown Perth provided overseas deposits services to customers through a number of channels including COD Macau (until October 2016) and Manila (until May 2017), and Company 10, based in South East Asia, from at least 1 January 2015 until September 2020. A number of High Risk Customers transacted through these channels, which often involved cash deposits being made by third parties. More than \$11 million moved through this channel.
- 361 As noted in paragraph 355(c), on and from 1 March 2016, Crown Melbourne and Crown Perth provided designated services to 60 high risk customers, without carrying out appropriate risk-based due diligence. As also noted in paragraph 355(c), during this period, turnover by these customers was in excess of \$70 billion⁹³ and revenue from these customers was about \$1,246 million.⁹⁴ Crown Melbourne and Crown Perth chose to continue business relationships with these high-risk customers, including high value customers with reported links to organised crime.
- 362 As noted in paragraph 355(d), a further 445 Crown customers were permitted to transact from 1 March 2016 to 30 April 2021 in ways that were indicative of ML/TF typologies. Many of those customers engaged in transactions totalling millions of dollars. Had Crown conducted appropriate risk-based customer due diligence, including appropriate risk-based transaction monitoring, this activity could have been identified and deterred sooner.

⁹³ For an explanation of turnover and its relationship to revenue and profit, see paragraphs 61 to 65.

⁹⁴ For an explanation of revenue and its relationship to profit, see paragraphs 63 to 65.

- 363 In respect of the customers referred to in paragraph 355 above, as noted in that paragraph:
- (a) Crown's failures exposed Crown and the Australian community to ML/TF risk; and
 - (b) had Crown appropriately monitored these customers, it may have identified activity indicative of ML/TF typologies sooner. Had this activity been identified sooner, it could have been investigated and, where determined to be suspicious, reported to AUSTRAC and law enforcement sooner, through SMRs. Had suspicious activity been identified sooner, Crown would have been in a position to undertake additional steps to identify, mitigate and manage the ongoing risks.
- 364 Non-transparent movement of money and, as noted in paragraphs 351(d) and 353(i) above, deficiencies in KYC records may inhibit the ability of law enforcement and AUSTRAC to trace money to its source. This may inhibit law enforcement investigations, prosecutions and the recovery of proceeds of crime. Where money can be moved quickly and across borders, it can be even more difficult to trace and recover. These issues were compounded by Crown Melbourne's and Crown Perth's failures to ensure appropriate systems and controls to fully and accurately report SMRs, TTRs and IFTIs. Crown Melbourne's and Crown Perth's conduct undermined the objectives of the Act.
- 365 The ML/TF risk management failures occurred in circumstances where Crown Melbourne and Crown Perth were operating a high turnover business. Between July 2015 and June 2020, Crown Melbourne generated the revenue figures outlined in subparagraph 349(h).
- 366 By failing to comply with the Act and Rules, Crown Melbourne and Crown Perth avoided expending funds that should have been invested in compliance including on IT, staffing and the development of AML/CTF controls. As noted in section H.7, significant funds have now been invested in those areas.

H.3 Prior contraventions

- 367 Crown Melbourne and Crown Perth have not previously been found to have engaged in any contravention of the AML/CTF Act.

H.4 Crown's size and financial position

- 368 In the period 1 March 2016 to June 2022, Crown Resorts was a publicly listed company. In June 2022, Crown Resorts was acquired by funds managed or advised by Blackstone Inc. (**Blackstone**) and its affiliates by way of a scheme of arrangement. The scheme consideration of \$13.10 for each share gave the company an implied equity value of \$8.9 billion and represented a premium of 32.3 per cent to the share price on the day before Crown Resorts announced the Blackstone acquisition proposal.
- 369 Following the acquisition, the Respondents, as wholly owned subsidiaries of Crown Resorts, became part of a consolidated group with Crown Resorts remaining as their parent entity (the **Crown Resorts Group**) and a newly-formed Blackstone controlled entity, SS Silver Pty Ltd, becoming the ultimate holding company of the Crown Resorts Group in Australia (**Crown Consolidated Group**).
- 370 The table below sets out relevant financial results of the Crown Resorts Group, Crown Melbourne and Crown Perth during the period Financial Year (**FY**) 2016 to FY2022.

(\$ million)	FY2016	FY2017	FY2018	FY2019	FY2020	FY2021	FY2022
Crown Resorts Group:							
Main Floor Gaming Revenue ⁹⁵	1,680.6	1,656.7	1,680.9	1,689.3	1,235.2	885.2	1,080.1
VIP Program Play Revenue (theoretical) ⁹⁶	986.5	548.5	758.2	568.3	306.7	6.9	16.9
VIP Program Play Revenue (actual)	1,004.6	605.3	739.9	593.3	440.1	3.5	13.3
Total Revenue (actual)	3,617.8	3,345.3	3,495.2	2,929.2	2,237.2	1,536.8	1,935.6
EBITDA (theoretical, before closure costs & significant items)	855.8	828.0	878.3	802.1	503.8	241.7	127.4
EBITDA (actual, before closure costs & significant items)	861.4	790.3	792.4	849.7	615.4	238.5	123.6
Closure Costs ⁹⁷	-	-	-	-	(107.3)	(171.4)	(113.1)
EBITDA related Significant Items ⁹⁸	-	-	-	-	(3.5)	47.0	(710.1)
EBITDA (reported)	861.4	790.3	792.4	849.7	504.6	114.1	(699.6)
NPAT (before significant items)	393.6	308.9	326.7	401.8	158.2	(207.0)	(111.3)
Significant Items	555.2	1,557.2	232.2	-	(78.7)	(54.6)	(834.1) ⁹⁹
NPAT (reported) ¹⁰⁰	948.8	1,866.1	558.9	401.8	79.5	(261.6)	(945.4)
Crown Melbourne							
Main Floor Gaming Revenue	1,183.3	1,182.7	1,217.0	1,235.1	890.6	406.9	650.7

⁹⁵ Does not include VIP program play revenue.

⁹⁶ Theoretical results have been adjusted to exclude the impact of any variance from theoretical win rate on VIP program play (at Crown Melbourne, Crown Perth (until 24 February 2021) and Crown Aspinalls). The theoretical win rate is the expected hold percentage on VIP program play over time. The theoretical result gives rise to adjustments to VIP program play revenue, operating expenses and income tax expense. Crown uses theoretical results to measure performance of the business as it removes the inherent volatility in VIP gaming revenue.

⁹⁷ Closure Costs reflect all costs incurred at Crown Melbourne, Crown Perth and Crown Sydney whilst the properties were closed due to Government direction.

⁹⁸ Significant items are transactions that are not in the ordinary course of business or are material and unexpected due to their size and nature.

⁹⁹ This figure includes significant one-off expenses, including \$617.2 million for regulatory and other matters (which included provisions for penalties and fines resulting from regulatory action, including a provision of \$360 million for this proceeding).

¹⁰⁰ Reported Net Profit after Tax attributable to equity holders of the parent.

(\$ million)	FY2016	FY2017	FY2018	FY2019	FY2020	FY2021	FY2022
VIP Program Play Revenue (theoretical)	676.5	340.3	591.8	441.4	224.9	4.4	-
Total Revenue (theoretical)	2,312.5	1,994.8	2,279	2,155.4	1,477.8	582.5	939.9
EBITDA (theoretical, before closure costs & significant items)	673.3	588.8	645	589.5	354.3	94.1	91.0
Closure Costs	-	-	-	-	(65.8)	(145.9)	(94.5)
EBITDA related Significant Items	-	-	-	-	-	(45.5)	(425.0)
EBITDA (theoretical)	673.3	588.8	645	589.5	288.5	(97.2)	(428.5)
Crown Perth							
Main Floor Gaming Revenue	497.3	474.0	463.9	454.2	344.6	478.3	429.4
VIP Program Play Revenue (theoretical)	202.8	109.3	103	72	49.5	0.4	-
Total Revenue (theoretical)	922	830.1	844.5	799.4	613.3	742.8	735.2
EBITDA (theoretical, before closure costs & significant items)	259.9	244.8	248.8	221.8	161.8	254.2	174.7
Closure Costs	-	-	-	-	(19.7)	(20.3)	(3.8)
EBITDA related Significant Items	-	-	-	-	-	(2.3)	(142.8)
EBITDA (theoretical)	259.9	244.8	248.8	221.8	142.1	231.6	28.1

371 FY2019 represents the last full financial year before COVID-19.

372 COVID-19 had a significant financial impact on Crown Resorts Group, including Crown Melbourne and Crown Perth, as indicated in the FY2020-2022 figures in the table.

373 The losses for FY2021 and FY2022 have primarily resulted from the significant impact of COVID-19 restrictions on the Crown Resorts Group's business operations when properties were closed to the public, including Closure Costs shown in the table above. Substantial costs and penalties (which also contributed to the losses) have arisen from the Royal Commissions and Commissions

of Inquiry that the Crown Resorts Group was the subject of in each of NSW, Victoria and Western Australia between 2020 and 2022 (as well as the other significant expenses noted as significant items above).

374 As at the end of FY2022, Crown Resorts Group had net assets of \$3,524 million. The Crown Consolidated Group had net assets of \$4,987 million.

375 As set out in the affidavit dated 30 May 2022, to be filed by Crown in these proceedings:

- (a) The challenging trading conditions facing the Crown Resorts Group subsist. At the December 2022 Board meeting, the Crown Resorts Group was forecasting a net loss after tax for FY2023 of \$(199) million, including third party interest costs of the Crown Consolidated Group (Forecast FY2023 Loss). The forecast was based on actual results to October 2022, with a re-forecast for November 2022 to June 2023. As a result, primarily, of poorer than expected trading conditions since the forecast was prepared (results for the November 2022 to March 2023 period were \$80 million below forecast), the Forecast FY2023 Loss is approximately \$(374) million. The Forecast FY2023 Loss will be further increased to the extent that the penalty in this proceeding and amounts for regulatory and other matters exceed the provisions recognised in the FY2022 financial statements.
- (b) As at 31 March 2023, the Crown Resorts Group had access to approximately \$441 million in cash through cash reserves (excluding cash in cages and on-floor) and access to a \$200 million working capital facility, which was fully drawn in April 2023 (except for approximately \$2 million). Due to the continued deterioration in the Crown Resorts Group's net cashflow position, that amount is presently forecast to be reduced to approximately \$325 million as at 30 June 2023. If subdued trading continues, liquidity will continue to deteriorate into FY2024.
- (c) Crown Resorts needs to maintain sufficient liquidity to ensure that it can continue as a going concern to be able to fund payroll and other ongoing obligations of the Crown Resorts Group, including casino duties and levies. In addition, liquidity needs to be sufficient to support potential business interruption events (such as those experienced through the pandemic), payment of regulatory penalties and other unanticipated costs. Crown Resorts' Treasury policy has been temporarily amended because of forecast declining cash reserves to reduce the minimum liquidity level (that is, cash and committed facilities) from \$400 million to \$250 million until 31 December 2023.
- (d) In the event that the forecast level of available cash and committed facilities as at 30 June 2023 is as forecast (being the approximately \$325 million referred to above), Crown Resorts will have a \$75 million buffer to its minimum liquidity level required to support ongoing operations.
- (e) The forecast cash position as at 30 June 2023 does not include the payment of (or part payment of) the pecuniary penalty in this proceeding, nor does it include payments the Crown Resorts Group may have to make to State gaming regulators for penalties and fines in respect of matters arising from the commissions of inquiry (in addition to those already made to the regulator in Victoria), or in respect of potential outstanding tax liabilities and legacy litigation. The timing of such payments (if required) is not presently known or able to be quantified, so they are not included within the current year forecast. If and when they crystallise, they are expected to result in a further compromise to the Crown Resorts Group's cash position.

H.5 Board and senior management involvement

- 376 The contraventions set out above were not a consequence of any deliberate intention to contravene the AML/CTF Act. At all times, the Crown boards and senior management sought to ensure that Crown would comply with its obligations under the AML/CTF Act.
- 377 Crown acknowledges that at all times during the Relevant Period the AML/CTF Act and AML/CTF Rules required that a reporting entity's Part A program must be subject to the ongoing oversight of each reporting entity's board and senior management. As part of this oversight, Crown's boards and senior management were responsible for oversight of the management of ML/TF risks faced by its business in accordance with the AML/CTF Act and AML/CTF Rules.
- 378 Between 1 March 2016 and 1 November 2020, as a result of the matters described in paragraph 138, Crown Melbourne and Crown Perth did not comply with section 84(2)(a) of the AML/CTF Act and part 8.4 of the AML/CTF Rules.
- 379 While improvements in the oversight framework for the Crown boards and senior management were adopted on and from 2 November 2020 until 1 March 2022, as a result of the matters described in paragraph 300(a), Crown Melbourne and Crown Perth did not comply with section 85(2)(a) of the AML/CTF Act and with part 9.4 of the AML/CTF Rules.
- 380 Since November 2020, the Crown boards and senior management have overseen a range of measures directed at improving Crown's AML/CTF function and the identification, mitigation, and management of ML/TF risks, including the measures outlined at H.7 below. These improvements have been directed at addressing, among other things, the shortcomings listed at paragraph 138 above. Crown acknowledges that these improvements could and should have been made earlier. Given the scale of the remediation required, it has taken significant time to exercise appropriate oversight of the AML/CTF Program.
- 381 In recognition of, among other matters, the importance of compliance with Crown's AML/CTF obligations and the significance of the breaches which are the subject of the proceedings, the Crown boards and senior management have been completely reconstituted. The new directors and senior management team have been subject to rigorous probity checks by the State-based gaming regulators, and have demonstrated a commitment to uplifting Crown's AML/CTF compliance framework and making Crown a leader in ML/TF risk management.

H.6 Cooperation with AUSTRAC and contrition

- 382 At all times during and since the Relevant Period, Crown has maintained a cooperative and constructive relationship with AUSTRAC, including cooperating fully with AUSTRAC compliance assessments and AUSTRAC's enforcement investigations. As part of this relationship, Crown has proactively shared information and reports with AUSTRAC concerning its compliance and program of reform.
- 383 Crown has also engaged constructively with AUSTRAC in relation to responding to the Statement of Claim. In particular, and in addition to the remediation, corrective measures and enhancements discussed in section H.7 below, Crown has:
- (a) continued to work cooperatively with AUSTRAC on matters relating to AUSTRAC's ongoing supervisory role and in the conduct of the Proceedings; and
 - (b) following the commencement of the Proceedings:
 - (i) promptly expressed contrition and its desire to work with AUSTRAC to resolve the Proceedings;

- (ii) initiated communication with AUSTRAC in relation to the mediation and participated in the mediation process; and
- (iii) admitted to contraventions of the relevant sections of the AML/CTF Act (sections 36 and 81) at the earliest available opportunity.

384 Crown:

- (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 casino, Crown plays a key role in combating money laundering and terrorism financing;
- (c) accepts its accountability for the admitted contraventions;
- (d) expresses its deep regret for those contraventions; and
- (e) acknowledges the significant impact that deficiencies in its systems and processes can have on efforts to combat money laundering and terrorism financing.

385 To demonstrate Crown's commitment to and leadership in ML/TF risk management, and in addition to the matters set out in section H.7 below, Crown has taken steps to improve its relationships with law enforcement and seek to become an industry leader on AML/CTF compliance. Steps taken include:

- (a) signed a memorandum of understanding on information sharing with the Australian Criminal Intelligence Commission and the Australian Federal Police;
- (b) leading in the establishment of the Australia/NZ Financial Crime Gambling Industry Forum, comprising key casino and gambling organisations. The purpose of the Forum is to drive industry engagement on ML/TF risk management, and other financial crime risks, as well as to facilitate a consistent industry approach; and
- (c) participating in the Fintel Alliance Casino Working Group aimed at identifying and responding to the ML/TF risks within casinos. The working group brings together financial crime leads from law enforcement, AUSTRAC and other government agencies with representatives of Australian casinos.

H.7 Remediation, corrective measures and enhancements

386 Since 2020 Crown has progressively uplifted its approach to the identification, mitigation and management of the ML/TF risk posed by the designated services it provides, responding to the issues and failures identified in this proceeding, as well as the three public inquiries conducted between 2020 and 2022.

387 Crown has already invested more than \$40 million in financial crime compliance since 2020, with a budget of \$27.9 million for FY2023, and further significant investment committed for future financial years. Enhancements have been made under a management-led program with Board oversight.

388 The program of reform is still in progress. For this reason, as at the date of filing, AUSTRAC has not been in a position to conduct a comprehensive assessment of Crown's remediation or its effectiveness.

389 Crown has regularly briefed AUSTRAC on its program of reform, including through periodic progress briefings and provision of key documents such as:

- (a) new versions of its Joint AML/CTF Program;
- (b) the reports of its 2021 and 2022 EWRA;
- (c) a copy of the independent review report referred to at paragraph 405; and
- (d) board papers outlining progress in implementing the program of reform.

390 The briefing that has been provided to AUSTRAC is summarised below and divided into the following categories:

- (a) Governance, oversight and resourcing;
- (b) enhancements to risk assessment capabilities, and risk-based systems and controls;
- (c) regulatory relationships and industry engagement; and
- (d) internal and external assurance.

H.7.1 Governance, oversight and resourcing

391 In late 2020, Crown established a Financial Crime team. The Financial Crime team has evolved over time and has an embedded three lines of defence model. This has resulted in a Line 2 Financial Crime Risk team (reporting to the Chief Legal and Compliance Officer) and a Line 1 Financial Crime Operations and Solutions team (reporting to the Group Casino Officer). The Line 2 Financial Crime Risk team remains independent of Crown's business units and, in particular, the AML/CTF Compliance Officer and the Financial Crime Risk team have a direct reporting line to the boards, including the Crown Resorts Board.

392 Crown has increased the team responsible for financial crime compliance from five full time employees in 2020 to 176 full time employees and contractors in April 2023, with new recruits bringing financial crime risk management experience from gambling, banking and law enforcement sectors to bolster its capabilities. Crown has also undertaken a significant uplift in financial crime training and staff awareness, including developing and facilitating training to all board members and senior management, analysing training needs, and completing data driven assessments of remedial training needs.

393 Crown adopted a new Joint AML/CTF Program on 2 November 2020, to ensure a consistent, group-wide approach to the identification, mitigation and management of ML/TF risks. This new Joint AML/CTF Program has been progressively improved with new versions adopted and implemented in 2021, 2022 and 2023. The current Joint AML/CTF Program has been informed by the two enterprise wide ML/TF risk assessments (**ML/TF EWRAs**) in late 2021 and early 2023 that Crown has completed, and is supported by:

- (a) improvements in governance and oversight, through new or improved board and senior management committees and reporting, with boards and senior management receiving better training and having stronger competencies in financial crime risk management;
- (b) uplifted processes and documentation for AML/CTF compliance, both within the first and second line;
- (c) enhanced and more targeted AML/CTF training for Crown's employees and contractors;
- (d) mapping obligations under the AML/CTF Act and AML/CTF Rules to accountabilities and responsibilities across Crown's executive management team, conducting business walkthroughs of their financial crime obligations, with documented end-to-end processes and controls; and

- (e) operational procedures, through its Policy Uplift Program, addressing the core elements of the Joint AML/CTF Program.
- 394 Two new financial crime committees, the Financial Crime Oversight Committee (**FCOC**) and the Financial Crime Working Group (**FCWG**) have been established to support oversight of the Joint AML/CTF Program;
- (a) FCOC membership comprises 'C' level executives across Crown Resorts and each reporting entity, and its primary function is to assist the Crown boards in fulfilling their ML/TF oversight responsibilities; and
 - (b) FCWG membership comprises senior Financial Crime team members, including the AML/CTF Compliance Officer, and Executive General Managers and General Managers from business units providing designated services along with key support departments. It has been established to support the FCOC to monitor and assess compliance with the obligations of Crown Resorts and each DBG entity.
- 395 Financial crime reporting to the Crown boards has also improved significantly, with the boards now receiving a Financial Crime Risk update and update on the status of Crown's program of reform as standalone items at each quarterly board meeting which, among other things, identify and analyse key operational metrics, and provide information in respect of all remediation activity.
- 396 Crown has also established the Transaction Monitoring Committee to provide oversight of Crown's TMP and introduced the Financial Crime Regulatory Event Forum, now the Financial Crime Breach Determination Forum. This assesses potential breaches of Crown's financial crime obligations, determines whether an actual breach occurred and, if so the materiality of the breach, and to which regulator it should be reported to.

H.7.2 Enhancements to risk assessment capabilities, and risk-based systems and controls

- 397 Crown has progressively been applying a stricter and more conservative risk mitigation from late 2020, including:
- (a) terminating all dealings with junkets and putting in place controls to ensure compliance with this policy;
 - (b) prohibiting third party transfers (including from money remitters) to and from its bank accounts (subject to very limited exceptions);
 - (c) prohibiting cash deposits into its bank accounts, introducing systems to identify cash deposits into bank accounts and mandatory return of cash deposits received;
 - (d) prohibiting the 'aggregation' of customer transactions into gaming accounts (a cause of structuring, smurfing and cuckoo smurfing being missed);
 - (e) implementing new limits on cash transactions at the Cage;
 - (f) implementing new customer review procedures, including the Significant Player Review and improving ECDD procedures;
 - (g) having a clearer articulation of customers with whom Crown does not wish to conduct business, implementing new policies and procedures to deal with the escalation (and potential exit) of these customers;

- (h) requiring source of funds declarations where transactions are over a certain limit and introducing new limits on customer identification requirements that go beyond what the AML/CTF Rules require; and
 - (i) updating the Crown Resorts Risk Appetite Statement (**RAS**) to address AML/CTF risk matters. The updated RAS provides, among other things, a clear articulation of qualitative statements and quantitative metrics in relation to ML/TF. It also includes additional risk sub-categories and a defined process for monitoring, reporting and escalating risk appetite breaches.
- 398 Crown's understanding of its ML/TF risk is maturing significantly across the paradigms of product, channel, customer, jurisdiction and employee risk, as well as at an enterprise wide level, having:
- (a) established and then improved and updated its ML/TF EWRA methodology to address recommendations from internal and external reviews. Crown also established a EWRA Design Authority as an oversight and decision-making forum which was chaired by Crown's AMLCO and included senior representatives and subject matter experts from Crown's Financial Crime team;
 - (b) undertaken two ML/TF EWRAs in each of 2021 and 2022 (with the 2022 ML/TF EWRA undertaken under the ML/TF EWRA Methodology using a digital tool), and having updated Parts A and B of its Joint AML/CTF Program several times to make enhancements and adjustments to reflect new systems and controls as well as the findings of both ML/TF EWRAs;
 - (c) designed and finalised a new and improved strategic customer risk assessment (**CRA**) methodology (based on an interim CRA implemented in Crown Sydney). Subject to relevant State gaming regulator approval, Crown expects the strategic CRA to be implemented across the Crown DBG by June 2023;
 - (d) implemented a new and improved jurisdiction risk assessment methodology;
 - (e) finalised the design of a new product risk assessment methodology and channel risk assessment methodology and related implementation procedures, with implementation having commenced; and
 - (f) finalised and released a new Risk and Control Framework which governs the development and maintenance of Risk and Control Self Assessments at Crown.
- 399 Crown has also introduced or enhanced existing controls to mitigate and manage identified ML/TF risks. In addition to the steps described at paragraph 397, Crown has, among other things:
- (a) uplifted its employee due diligence framework;
 - (b) introduced an automated reconciliation process for matching patron deposits through Crown's bank accounts to the patron accounts in Crown's gaming management system and in the process, highlight exceptions for further action;
 - (c) introduced the collection of mandatory KYC information, including citizenships held, occupation and residential address;
 - (d) introduced enhanced controls over peer-to-peer poker in Melbourne and Perth;
 - (e) implemented a limit on uncarded cash buy-ins for table games, set at \$4,999; and

- (f) uplifted its OCDD framework by finalising and operationalising a periodic ECDD refresh plan for existing high and significant risk customers, completing a strategic assessment across the three lines of defence, finalising a new KYC refresh strategy and developing reporting dashboards to support identification of banned/exited customers.
- 400 As part of its uplift in controls, Crown has made a series of significant investments and changes to its technology, including:
- (a) implementing a digital governance, risk and compliance tool, which integrates with Crown's systems to allow Crown to more effectively manage end-to-end obligations, appropriately respond to its regulatory commitments and support key functions like internal audit, assurance, risk and compliance;
 - (b) introducing a risk-based automated transaction monitoring system which consists of 25 rules addressing ML/TF typologies in the areas of customer behaviour, financial and cash transactions;
 - (c) implementing key features of a new case management system and reporting dashboard that more effectively identifies transaction monitoring insights, coverage gaps and uplift opportunities;
 - (d) introducing various new technical platforms which enhance Crown's customer due diligence and ECDD capabilities such as in customer screening, verification of sources of wealth/funds, and identification of internal and external customer networks;
 - (e) digitising the internal reporting of unusual activity by frontline staff; and
 - (f) adopting an electronic digital verification service for use in OCDD.
- 401 Crown has advised AUSTRAC that the control enhancements include an improved number of unusual activity reports made internally and an improved rate of review of UARs.

H.7.3 Regulatory relationships and industry engagement

- 402 Refer to Section H.6 at paragraphs 382 to 385.

H.7.4 Internal and external assurance

- 403 Crown has established a Risk Assurance function (which covers both Financial Crime and other areas of risk at Crown) which has:
- (a) defined Crown's AML/CTF obligations;
 - (b) cascaded the AML/CTF obligations, accountabilities and responsibilities across Crown's executive management team;
 - (c) conducted business walkthroughs of their financial crime obligations, with documented end-to-end processes and controls; and
 - (d) completed current state assessments of the controls over Crown's AML/CTF obligations including ML/TF risk assessment, transaction monitoring, transaction reporting, customer onboarding (including ACIP, additional KYC collection and refresh, and customer screening), AML/CTF governance obligations, and Crown's employee obligations. The results of these assessments have fed into the ML/TF EWRA's.
- 404 Following the numerous public inquiries which have considered matters relevant to management of ML/TF risk, Crown has been, and continues to be, subject to a significant level of review and scrutiny by third parties in relation to AML and its program of reform in relation to

financial crime. Crown has advised AUSTRAC that, in the case of each external review, Crown has accepted each of the recommendations and incorporated them into its program of reform, with an assurance process over implementation of agreed actions.

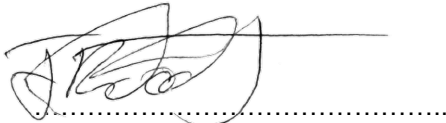
- 405 Crown's Joint AML/CTF Program has also been subject to external independent review. This external assurance includes two independent reviews conducted pursuant to part 9.6 of the AML/CTF Rules. The first independent review was completed on 31 March 2022 and a copy was provided to AUSTRAC. The second independent review was completed on 22 May 2023 and a copy of the independent review report has been shared with AUSTRAC. Crown has incorporated recommendations from the first review and will incorporate recommendations from the second review into its program of reform.

H.8 Other facts relevant to deterrence

- 406 Crown is now wholly owned by a new shareholder, being entities owned by funds managed or advised by Blackstone Inc. and its affiliates.
- 407 Crown has already suffered significant financial and reputational loss for the conduct the subject of this proceeding as a result of three previous public inquiries, other regulatory proceedings and a class action in which its AML/CTF failings have featured prominently.
- 408 As a result of the three public inquiries, Crown Melbourne, Crown Perth and Crown Sydney were each found to be unsuitable to hold a casino licence, and the casino licences in each State in which Crown operates were made conditional on certain steps being taken, including in relation to AML/CTF, with the threat of licence cancellation if these steps are not taken to the satisfaction of State regulators. The processes with the State regulators involve external third parties reviewing the sufficiency and effectiveness of the steps Crown is taking and providing reports to the State regulator that will inform the decision as to whether to cancel Crown's licence. These external third parties include:
- (a) a Special Manager appointed under the *Casino Control Act 1991* (Vic) for a two year term, with all the powers, rights and privileges of a director, including the right to attend board meetings and to access all books and records of Crown Melbourne, but also with unique coercive powers, including the power to direct Crown Melbourne to do, or to refrain from doing, any act; and
 - (b) an independent monitor appointed under the *Casino Legislation Amendment (Burswood Casino) Act 2022* (WA) to supervise and review Crown Perth's remediation over a two year period.
- 409 While they were not fines for contraventions of the AML/CTF Act, between 2021 and 2023, Crown has been subject to fines by the Victorian Gambling and Casino Control Commission (VGCCC) arising from contraventions that are also concerned with Crown's failure to guard against criminal exploitation of its Melbourne casino. The VGCCC has issued Crown Melbourne with fines as follows:
- (a) A fine of \$1 million issued in April 2021 for failure to implement a robust process to consider the ongoing probity of its junkets in the period January 2016 to 2020, in contravention of section 121(4) of the CCA. The VGCCC took into account, as one of a number of aggravating factors when determining penalty, that an objective of the CCA was to ensure that the operation of the Melbourne casino remained free from criminal influence or exploitation (**Victorian CCA Objective**) and that Crown continuing to engage with junket operators and players was inconsistent with that objective;

- (b) A fine of \$80 million issued on 27 May 2022 for practices in the period 2012 to 2016 relating to the Hotel Card channel that contravened section 68(2)(c) of the CCA, which prohibits a casino providing money or chips as part of a transaction involving a credit card, and record keeping requirements in section 124 of the CCA. Crown conceded that it was not far-fetched to imagine that organised crime figures took advantage of these practices and may have involved Crown Melbourne dealing with the proceeds of crime, and that the practices may have involved Crown Melbourne dealing with the proceeds of crime. The VGCCC took these matters into account as significant matters of aggravation, particularly having regard to the Victorian CCA Objective; and
- (c) A fine of \$30 million issued on 26 April 2023 for practices relating to bank cheques and blank cheques that contravened credit betting prohibitions in section 68 of the CCA in the period since Crown commenced operations up until 2021. The VGCCC took into account, as one of a number of aggravating factors when determining penalty, that the practices were likely to have resulted in criminal infiltration by money launderers.

Date: 30 May 2023



James Docherty

AGS Lawyer

For and on behalf of the Australian Government Solicitor

Lawyer for the Applicant



Peter Haig and Christopher Kerrigan

Solicitors for the Respondents

Schedule 1 – Private / VIP gaming locations

Venue name	Access	Location
Teak Room (also known as Pit 86)	Accessed by Crown Rewards members who held Gold Tier accounts or above	Crown Melbourne
Mahogany Room (also known as Pit 38 and inclusive of Ultra Black and Black Salons)	Accessed by Crown Rewards members who held Platinum Tier accounts or above, or Mahogany Gold members by invitation. Only Black Tier customers had access to the Ultra Black and Black Salons	Crown Melbourne
Mahogany Lounge (from 2019 onwards)	Accessed by Crown Rewards members who held Platinum Tier accounts or above	Crown Melbourne
Mahogany Suites (from January 2020 onwards)	Accessed by Crown Rewards members who held Black Tier accounts or above	Crown Melbourne
Private gaming salons	Accessed by Crown Rewards members who held Black Tier accounts or above	Crown Melbourne and Crown Perth
Riverside Room	Accessed by Crown Rewards members who held Silver Tier accounts or above (noting at Crown Melbourne from late 2021, access was granted to all customers regardless of membership tier). In addition, at Crown Perth, players on junket programs or premium player programs could also access the Riverside Room	Crown Melbourne and Crown Perth
Pearl Room	Accessed by customers with Pearl Room membership (PR membership) and their guests, VIP players on premium player programs and junket programs, and Gold, Platinum or Black Tier status Crown Rewards members who maintained a turnover of \$100,000 annually, earned a minimum of 40 status credits through gaming activity and completed an Expression of Interest form	Crown Perth
Diamond Room (from 26 November 2018)	Accessed by customers with PR membership and their guests	Crown Perth
80 Series Salons	Accessed by customers with PR membership and their guests, and customers playing under a premium player program or junket program with front money of at least \$2 million	Crown Perth
Sky Salon	Accessed by customers with PR membership and their guests, and customers playing under a premium player program or junket program with front money of at least \$2 million	Crown Perth
Crown Towers Salons (from 1 December 2016)	Accessed by customers with PR membership and their guests, and customers playing under a premium player program or junket program with front money of at least \$2 million	Crown Perth
The Suite	Accessed by customers by invitation only	Crown Perth

Schedule 2 – ML/TF vulnerabilities, techniques and typologies

A. Structuring

- 410 Structuring is the deliberate division of a large amount of cash into smaller deposits to avoid the reporting threshold in section 43 of the AML/CTF Act. Section 43 of the AML/CTF Act requires a reporting entity to give the AUSTRAC CEO a report of a transaction in circumstances where a reporting entity provides (or commences to provide) a designated service to a customer and the provision of the service involves a threshold transaction. A threshold transaction is defined under section 5 of the AML/CTF Act as meaning a transaction involving the transfer of physical currency, where the total amount transferred is not less than \$10,000.

B. Cuckoo smurfing/smurfs

- 411 Cuckoo smurfing is a method of money laundering used by criminals to move funds across borders and make money generated by their illegal activities appear to have come from a legitimate source. Cuckoo smurfing is facilitated by professional money laundering syndicates who work with a corrupt remitter based overseas, as follows:
- (a) the corrupt remitter accepts an instruction from a customer to make a payment to an Australian-based beneficiary customer;
 - (b) the corrupt remitter hijacks the money transfer to the Australian-based beneficiary by replacing the funds the subject of that transfer with (different) funds which are sourced from criminal activity;
 - (c) a smurf or third party agent deposits cash into Australian bank accounts on behalf of a money laundering syndicate controller; and
 - (d) the international transfer is offset without the physical movement of funds.
- 412 A 'smurf' or a 'third party agent' is an individual conducting cash deposits into Australian bank accounts on behalf of a money laundering syndicate controller. Junket operators may act as remitters and may facilitate cuckoo smurfing.

C. Offsetting

- 413 Offsetting enables an international transfer of value to occur without actually transferring money. This is possible because the arrangement involves a financial credit and debit (offsetting) relationship between two or more persons operating in different countries. Criminals can exploit offsetting to conceal the amount of illicit funds transferred, obscure the identity of those involved and avoid reporting to AUSTRAC.

D. Loans or credit

- 414 Loans or credit can be used to launder funds. Loans can be taken out as a cover for laundering criminal proceeds under the guise of repayments, including by lump sum cash payments, smaller structured cash amounts or offsetting.

E. Third parties

- 415 Customers of casinos may seek to use third parties to obtain designated services on their behalf. Third parties may also seek to deposit money into a customer's gaming account. A customer may seek to transfer money from their gaming account to a third party. The involvement of third-parties in transactions such as these can distance customers from illicit funds, disguise ownership of funds and complicate asset confiscation efforts by authorities.

F. Minimal or no gaming activity

- 416 Money deposited with a casino or exchanged for CVIs (including chips and tickets) and then withdrawn with minimal or no gaming activity may indicate ML/TF activity, despite the money appearing to have a legitimate origin. Little money is risked in this scenario. Gaming losses sustained by a customer, even if minimal, can give the incorrect appearance that the customer is engaging in genuine gaming activity.

G. High turnover or high losses

- 417 Gaming involving high turnover or high losses may indicate unusual or suspicious activity and may raise questions about the customer's source of wealth or funds.
- 418 Gaming involving escalating rates of high turnover or high losses may indicate unusual or suspicious activity and may raise questions about the customer's source of wealth or funds.
- 419 High turnover offers further opportunities for the placement and layering of illicit funds. This is a particular problem with junkets, where funds are pooled and the payment of winnings is facilitated by the junket operator. The problem is exacerbated where cash can be brought into private gaming rooms by unknown persons who are not junket players.

H. Specific casino games

- 420 Games that have a low house edge can be attractive to money launderers, as they offer the opportunity to launder large amounts with minimised losses. The house edge describes the mathematical advantage that a game, and therefore the casino, has over the customer with play over time.
- 421 Where games permit even-money wagering (such as roulette and baccarat), two customers can cover both sides of an even bet to give the appearance of legitimate gaming activity while minimising losses.
- 422 Games that permit rapid turnover of cash or CVIs are vulnerable to money laundering. This vulnerability is exacerbated where the game is automated and not face-to-face.

I. Misuse of CVIs

- 423 Chips and other CVIs are highly transferable and may be handed over to third parties or removed from casinos and used as currency by criminal groups, or taken out of the jurisdiction as a means of transferring value. The chips may be returned to the casino by third parties and cashed out, including in amounts below a reporting threshold. Individuals may also purchase CVIs from other customers using illegitimate funds and winnings, which are subsequently claimed from the Cage.

J. Bank cheques

- 424 The acceptance of bank cheques made out to casinos may facilitate money laundering. Bank cheques are essentially anonymised, as the casino cannot identify the source of the funds. A customer may use the bank cheque to purchase CVIs, which may then be converted to cash.

K. Bill stuffing

- 425 Bill stuffing involves a customer putting cash into an electronic gaming machine, collecting tickets with nominal gaming activity and then cashing out or asking for a cheque.

L. Refining

- 426 Refining can be indicative of ML/TF activity. Refining involves changing an amount of money from smaller denomination bills into larger denomination bills.

M. Loan sharking

- 427 Loan sharking is when a person lends money in exchange for its repayment at an excessive interest rate, and may involve intimidating or illegal methods to obtain repayment. Although there is no specific offence for loan sharking, the conduct of a loan shark may breach other laws.

N. Parking

- 428 Money may be parked in gaming accounts. Parking of illicit money puts distance between the act or acts that generated the illicit funds and the ultimate recipients of those funds, making it harder to understand or trace the flow of money. Gaming accounts can be used to park funds outside the banking system and to hide funds from law enforcement and relevant authorities.

Appendix 1 – High Risk Customers

Customer	Date customer first became a customer of Crown Melbourne	Date customer first became a customer of Crown Perth	Date customer ceased to be a customer of Crown Melbourne	Date customer ceased to be a customer of Crown Perth
Customer 1	04/09/2009	29/06/2010	22/01/2021	29/01/2021
Customer 2	25/05/2009	17/08/2009	22/01/2021	29/01/2021
Customer 3	09/12/2014	17/08/2009	22/01/2021	29/01/2021
Customer 4	31/05/2008	06/04/2010	-	-
Customer 5	23/02/2007	03/10/2006	22/06/2021	22/06/2021
Customer 6	07/01/2006	26/09/2014	20/11/2020	20/11/2020
Customer 7	15/07/2015		22/01/2021	
Customer 8	09/09/2007		22/01/2021	
Customer 9	08/06/2011		22/01/2021	
Customer 10	26/02/2007		22/01/2021	
Customer 11	20/09/2015	10/01/2015	20/01/2021	16/02/2021
Customer 12	03/10/2015	24/05/2016	20/01/2021	29/01/2021
Customer 13	07/02/2011	-	22/01/2021	
Customer 14	30/08/2017	-	22/01/2021	
Customer 15	26/04/1996	09/02/2002	-	-
Customer 16	29/04/2017	29/04/2017	-	-
Customer 17	26/09/1996	16/01/2015	-	-
Customer 18	27/10/2015	05/08/2006	-	-
Customer 19	03/02/2009	02/10/2015	-	-
Customer 20	06/08/2015		22/01/2021	
Customer 21	03/08/2000	-	-	-
Customer 22	16/06/2015	-	16/09/2021	-
Customer 23	05/04/2016	-	16/12/2019	-
Customer 24	21/12/2014	-	18/12/2019	23/12/2021
Customer 25	22/11/2014		-	-
Customer 26	9/06/1996	29/12/2016	15/08/2019	29/06/2020
Customer 27	26/07/2004	-		-
Customer 28	07/02/2000	-	-	-
Customer 29	06/04/2007	01/12/2011	20/01/2021	-
Customer 30	31/08/2009	-	16/12/2020	-

Customer	Date customer first became a customer of Crown Melbourne	Date customer first became a customer of Crown Perth	Date customer ceased to be a customer of Crown Melbourne	Date customer ceased to be a customer of Crown Perth
Customer 31	09/05/1998	11/06/1997	-	-
Customer 32	25/06/2008	26/06/2008	02/11/2020	03/11/2021
Customer 33	28/11/2015	-	-	-
Customer 34	28/10/2005		25/05/2021	
Customer 35	28/10/1999	-		-
Customer 36	22/09/1996	02/1996	22/06/2021	22/06/2021
Customer 37	01/02/2006		-	-
Customer 38	22/03/2012	17/11/2016	29/08/2020	31/08/2021
Customer 39	04/06/2007		30/07/2020	
Customer 40	06/02/2013		30/07/2020	
Customer 41	14/07/2012	-	-	-
Customer 42		01/05/2014	-	-
Customer 43	12/04/2012	21/07/2014	04/02/2020	31/01/2020
Customer 44	14/07/2000	07/05/2004	-	-
Customer 45	15/02/2018	08/08/2017	-	-
Customer 46	09/06/1993		22/01/2021	
Customer 47	22/06/2012	26/06/2012	19/11/2019	15/09/2021
Customer 48	02/09/2010		-	-
Customer 49	09/06/2000	-	-	-
Customer 50	09/04/2004		-	-
Customer 51	11/02/2012	-	02/08/2021	
Customer 52	04/02/2011		-	-
Customer 53	13/07/2017	29/03/2019	-	-
Customer 54	04/04/2018		13/05/2021	
Customer 55		18/08/2010	-	-
Customer 56	27/09/2013	-	20/05/2016	-
Customer 57	24/04/1996	-	05/12/2019	-
Customer 58	03/07/2016	-	08/06/2021	
Customer 59	01/01/2006	-	23/11/2020	
Customer 60	30/06/1994	-	10/12/2019	-

Appendix 2 – Typology Customers

Customer	Date DAB/SKA was opened ¹⁰¹	Crown Melbourne / Crown Perth
Customer 61	01/03/2016	Crown Melbourne
Customer 62	01/03/2016	Crown Perth
Customer 63	01/03/2016	Crown Melbourne
Customer 64	13/09/2019	Crown Perth
Customer 65	01/03/2016	Crown Melbourne and Crown Perth
Customer 66	4/12/2016	Crown Melbourne
Customer 67	01/03/2016	Crown Melbourne
Customer 68	01/03/2016	Crown Melbourne
Customer 69	04/08/2019	Crown Melbourne
Customer 70	01/03/2016	Crown Perth
Customer 71	01/03/2016	Crown Melbourne
Customer 72	01/03/2016	Crown Melbourne
Customer 73	01/03/2016	Crown Perth
Customer 74	01/03/2016	Crown Melbourne
Customer 75	01/03/2016	Crown Melbourne and Crown Perth
Customer 76	05/04/2019	Crown Melbourne
Customer 77	01/03/2016	Crown Melbourne
Customer 78	04/02/2018	Crown Perth
Customer 79	01/03/2016	Crown Perth
Customer 80	18/10/2018	Crown Melbourne
Customer 81	01/03/2016	Crown Perth
Customer 82	01/03/2016	Crown Melbourne
Customer 83	04/12/2018 (Crown Melbourne) 01/03/2016 (Crown Perth)	Crown Melbourne and Crown Perth
Customer 84	01/03/2016	Crown Melbourne
Customer 85	23/05/2019	Crown Melbourne
Customer 86	20/03/2019	Crown Melbourne

¹⁰¹ If opened prior to the start of the relevant period, being 1 March 2016, the start of the relevant period has been used as the applicable date.

Customer	Date DAB/SKA was opened ¹⁰¹	Crown Melbourne / Crown Perth
Customer 87	04/02/2020	Crown Perth
Customer 88	11/01/2020	Crown Melbourne
Customer 89	13/11/2019	Crown Perth
Customer 90	10/01/2019	Crown Melbourne
Customer 91	15/03/2019	Crown Melbourne
Customer 92	01/03/2016	Crown Perth
Customer 93	01/03/2016	Crown Melbourne
Customer 94	26/08/2016	Crown Melbourne
Customer 95	01/03/2016	Crown Melbourne
Customer 96	01/03/2016	Crown Melbourne
Customer 97	01/03/2016	Crown Melbourne
Customer 98	01/03/2016	Crown Melbourne
Customer 99	01/03/2016	Crown Melbourne
Customer 100	03/03/2020 (Crown Melbourne) 03/04/2020 (Crown Perth)	Crown Melbourne and Crown Perth
Customer 101	01/03/2016	Crown Melbourne
Customer 102	01/03/2016	Crown Perth
Customer 103	01/03/2016	Crown Melbourne
Customer 104	01/03/2016	Crown Melbourne
Customer 105	01/03/2016	Crown Melbourne
Customer 106	12/04/2016	Crown Melbourne
Customer 107	19/01/2020	Crown Melbourne
Customer 108	01/03/2016	Crown Melbourne
Customer 109	20/05/2016	Crown Melbourne
Customer 110	01/03/2016	Crown Perth
Customer 111	01/03/2016	Crown Melbourne
Customer 112	01/03/2016	Crown Melbourne
Customer 113	01/03/2016	Crown Melbourne
Customer 114	09/12/2017	Crown Melbourne
Customer 115	19/06/2018	Crown Melbourne

Customer	Date DAB/SKA was opened ¹⁰¹	Crown Melbourne / Crown Perth
Customer 116	21/03/2017 (Crown Melbourne) 02/03/2018 (Crown Perth)	Crown Melbourne and Crown Perth
Customer 117	01/03/2016	Crown Melbourne
Customer 118	01/03/2016	Crown Perth
Customer 119	01/03/2016	Crown Perth
Customer 120	01/03/2016	Crown Perth
Customer 121	19/12/2018	Crown Melbourne
Customer 122	01/03/2016	Crown Perth
Customer 123	13/07/2019	Crown Perth
Customer 124	01/03/2016	Crown Melbourne
Customer 125	01/03/2016	Crown Melbourne
Customer 126	16/05/2019	Crown Melbourne
Customer 127	28/10/2018	Crown Perth
Customer 128	23/04/2019	Crown Melbourne
Customer 129	01/03/2016	Crown Melbourne and Crown Perth
Customer 130	17/09/2016	Crown Melbourne
Customer 131	01/03/2016	Crown Melbourne
Customer 132	01/03/2016	Crown Melbourne and Crown Perth
Customer 133	13/08/2016	Crown Perth
Customer 134	01/03/2016	Crown Perth
Customer 135	16/05/2017	Crown Melbourne
Customer 136	01/03/2016	Crown Perth
Customer 137	01/03/2016	Crown Melbourne
Customer 138	01/03/2016	Crown Melbourne
Customer 139	10/07/2016	Crown Melbourne
Customer 140	31/08/2016	Crown Perth
Customer 141	01/03/2016	Crown Melbourne
Customer 142	01/03/2016	Crown Perth
Customer 143	01/03/2016	Crown Melbourne
Customer 144	01/09/2016	Crown Melbourne

Customer	Date DAB/SKA was opened ¹⁰¹	Crown Melbourne / Crown Perth
Customer 145	04/05/2019	Crown Melbourne
Customer 146	01/03/2016	Crown Melbourne
Customer 147	24/02/2018	Crown Perth
Customer 148	01/03/2016	Crown Melbourne
Customer 149	04/10/2019	Crown Melbourne
Customer 150	01/03/2016	Crown Melbourne
Customer 151	01/03/2016	Crown Perth
Customer 152	01/03/2016	Crown Melbourne
Customer 153	01/03/2016	Crown Melbourne
Customer 154	01/03/2016	Crown Melbourne
Customer 155	24/02/2019	Crown Melbourne
Customer 156	01/03/2016	Crown Melbourne
Customer 157	06/08/2017	Crown Melbourne
Customer 158	01/03/2016	Crown Melbourne
Customer 159	01/03/2016	Crown Perth
Customer 160	20/09/2019	Crown Perth
Customer 161	01/03/2016	Crown Melbourne
Customer 162	17/08/2019	Crown Perth
Customer 163	01/03/2016	Crown Melbourne
Customer 164	01/03/2016	Crown Melbourne
Customer 165	01/03/2016	Crown Melbourne
Customer 166	29/01/2017	Crown Melbourne
Customer 167	01/03/2016	Crown Melbourne
Customer 168	01/03/2016	Crown Melbourne
Customer 169	21/10/2017	Crown Melbourne
Customer 170	01/03/2016	Crown Melbourne
Customer 171	10/05/2018	Crown Perth
Customer 172	01/03/2016	Crown Perth
Customer 173	01/03/2016	Crown Perth
Customer 174	20/09/2017	Crown Melbourne
Customer 175	01/03/2016	Crown Melbourne

Customer	Date DAB/SKA was opened¹⁰¹	Crown Melbourne / Crown Perth
Customer 176	01/03/2016	Crown Melbourne
Customer 177	01/03/2016	Crown Perth
Customer 178	01/03/2016	Crown Melbourne and Crown Perth
Customer 179	01/03/2016	Crown Melbourne
Customer 180	01/03/2016	Crown Perth
Customer 181	01/03/2016	Crown Melbourne
Customer 182	01/03/2016	Crown Melbourne
Customer 183	01/03/2016	Crown Melbourne
Customer 184	05/06/2016	Crown Melbourne
Customer 185	29/02/2020	Crown Melbourne
Customer 186	01/03/2016	Crown Melbourne
Customer 187	17/07/2019	Crown Melbourne
Customer 188	01/03/2016	Crown Perth
Customer 189	01/03/2016	Crown Perth
Customer 190	01/03/2016	Crown Perth
Customer 191	01/03/2016	Crown Melbourne
Customer 192	01/03/2016	Crown Perth
Customer 193	01/03/2016	Crown Melbourne
Customer 194	01/03/2016	Crown Melbourne
Customer 195	08/09/2017	Crown Melbourne
Customer 196	04/02/2017	Crown Melbourne
Customer 197	01/03/2016	Crown Melbourne
Customer 198	01/03/2016	Crown Melbourne
Customer 199	01/03/2016	Crown Melbourne
Customer 200	01/03/2016	Crown Melbourne
Customer 201	01/03/2016	Crown Perth
Customer 202	25/12/2017	Crown Melbourne
Customer 203	03/04/2021	Crown Melbourne
Customer 204	01/03/2016	Crown Perth
Customer 205	01/03/2016	Crown Perth

Customer	Date DAB/SKA was opened ¹⁰¹	Crown Melbourne / Crown Perth
Customer 206	01/03/2016	Crown Melbourne
Customer 207	01/03/2016	Crown Melbourne
Customer 208	01/03/2016	Crown Melbourne
Customer 209	01/03/2016	Crown Melbourne
Customer 210	01/03/2016	Crown Melbourne
Customer 211	01/03/2016	Crown Melbourne
Customer 212	01/03/2016	Crown Melbourne
Customer 213	05/03/2020	Crown Perth
Customer 214	30/08/2019	Crown Melbourne
Customer 215	29/11/2019	Crown Melbourne
Customer 216	01/03/2016	Crown Melbourne
Customer 217	01/03/2016	Crown Melbourne
Customer 218	2/11/2019	Crown Perth
Customer 219	01/03/2016	Crown Perth
Customer 220	01/03/2016	Crown Perth
Customer 221	01/03/2016	Crown Melbourne
Customer 222	01/03/2016	Crown Melbourne
Customer 223	07/12/2018	Crown Perth
Customer 224	01/03/2016	Crown Perth
Customer 225	01/03/2016	Crown Melbourne
Customer 226	26/02/2020 (Crown Melbourne) 01/03/2016 (Crown Perth)	Crown Melbourne and Crown Perth
Customer 227	01/03/2016	Crown Melbourne
Customer 228	01/03/2016	Crown Melbourne
Customer 229	01/03/2016	Crown Perth
Customer 230	01/03/2016	Crown Melbourne
Customer 231	01/03/2016	Crown Perth
Customer 232	01/03/2016	Crown Melbourne
Customer 233	01/03/2016	Crown Melbourne
Customer 234	01/03/2016	Crown Perth
Customer 235	01/03/2016	Crown Melbourne

Customer	Date DAB/SKA was opened¹⁰¹	Crown Melbourne / Crown Perth
Customer 236	19/05/2019	Crown Perth
Customer 237	01/03/2016	Crown Melbourne
Customer 238	01/03/2016	Crown Perth
Customer 239	29/12/2020	Crown Melbourne
Customer 240	10/02/2020	Crown Perth
Customer 241	24/11/2017	Crown Melbourne
Customer 242	01/03/2016	Crown Perth
Customer 243	3/06/2016	Crown Melbourne
Customer 244	29/07/2016	Crown Melbourne
Customer 245	01/03/2016	Crown Melbourne
Customer 246	11/04/2017	Crown Melbourne
Customer 247	01/03/2016	Crown Melbourne
Customer 248	14/05/2017	Crown Melbourne
Customer 249	01/03/2016	Crown Melbourne
Customer 250	01/03/2016	Crown Melbourne
Customer 251	02/12/2016	Crown Melbourne
Customer 252	01/03/2016	Crown Melbourne
Customer 253	01/03/2016	Crown Perth
Customer 254	01/03/2016	Crown Melbourne
Customer 255	22/10/2016	Crown Melbourne
Customer 256	01/03/2016	Crown Melbourne
Customer 257	01/03/2016	Crown Perth
Customer 258	09/07/2018	Crown Melbourne
Customer 259	01/03/2016	Crown Melbourne and Crown Perth
Customer 260	01/03/2016	Crown Melbourne and Crown Perth
Customer 261	11/06/2019	Crown Melbourne
Customer 262	01/03/2016	Crown Melbourne
Customer 263	01/03/2016	Crown Melbourne
Customer 264	18/02/2018	Crown Melbourne
Customer 265	28/10/2017	Crown Perth

Customer	Date DAB/SKA was opened¹⁰¹	Crown Melbourne / Crown Perth
Customer 266	01/03/2016	Crown Melbourne
Customer 267	13/08/2018	Crown Perth
Customer 268	01/03/2016	Crown Perth
Customer 269	01/03/2016	Crown Perth
Customer 270	15/07/2019	Crown Melbourne
Customer 271	21/04/2016	Crown Perth
Customer 272	01/03/2016	Crown Melbourne
Customer 273	01/03/2016	Crown Melbourne
Customer 274	30/05/2019	Crown Melbourne
Customer 275	01/03/2016	Crown Perth
Customer 276	01/03/2016	Crown Melbourne
Customer 277	01/03/2016	Crown Melbourne
Customer 278	06/12/2016	Crown Perth
Customer 279	01/03/2016	Crown Melbourne
Customer 280	19/06/2019	Crown Perth
Customer 281	1/10/2019	Crown Melbourne
Customer 282	01/03/2016	Crown Melbourne
Customer 283	01/03/2016	Crown Melbourne
Customer 284	01/03/2016	Crown Melbourne
Customer 285	05/07/2016	Crown Melbourne
Customer 286	05/04/2019	Crown Melbourne
Customer 287	06/09/2019	Crown Melbourne
Customer 288	01/03/2016	Crown Perth
Customer 289	11/12/2016	Crown Melbourne
Customer 290	01/03/2016	Crown Melbourne
Customer 291	05/10/2019	Crown Melbourne
Customer 292	01/03/2016	Crown Melbourne
Customer 293	01/03/2016	Crown Perth
Customer 294	01/03/2016	Crown Melbourne
Customer 295	01/03/2016	Crown Perth
Customer 296	23/06/2018	Crown Melbourne

Customer	Date DAB/SKA was opened¹⁰¹	Crown Melbourne / Crown Perth
Customer 297	01/03/2016	Crown Melbourne
Customer 298	01/03/2016	Crown Melbourne
Customer 299	30/03/2018	Crown Melbourne
Customer 300	01/03/2016	Crown Melbourne
Customer 301	01/03/2016	Crown Melbourne
Customer 302	21/10/2019	Crown Melbourne
Customer 303	10/06/2017	Crown Melbourne
Customer 304	11/07/2019	Crown Melbourne
Customer 305	01/03/2016	Crown Perth
Customer 306	01/03/2016	Crown Melbourne and Crown Perth
Customer 307	01/03/2016	Crown Perth
Customer 308	10/12/2017	Crown Perth
Customer 309	13/02/2019	Crown Perth
Customer 310	01/03/2016	Crown Perth
Customer 311	01/03/2016	Crown Perth
Customer 312	01/03/2016	Crown Perth
Customer 313	08/04/2019	Crown Perth
Customer 314	14/02/2020	Crown Perth
Customer 315	01/03/2016	Crown Melbourne
Customer 316	22/02/2020	Crown Perth
Customer 317	01/11/2018	Crown Melbourne
Customer 318	01/03/2016	Crown Perth
Customer 319	01/03/2016	Crown Melbourne
Customer 320	01/03/2016	Crown Melbourne
Customer 321	01/03/2016	Crown Perth
Customer 322	03/05/2017	Crown Melbourne
Customer 323	01/03/2016	Crown Melbourne
Customer 324	01/03/2016	Crown Melbourne
Customer 325	01/03/2016	Crown Melbourne
Customer 326	07/12/2018	Crown Perth

Customer	Date DAB/SKA was opened ¹⁰¹	Crown Melbourne / Crown Perth
Customer 327	01/03/2016	Crown Melbourne
Customer 328	01/03/2016	Crown Melbourne
Customer 329	24/01/2020	Crown Melbourne
Customer 330	01/03/2016	Crown Melbourne
Customer 331	01/03/2016	Crown Melbourne
Customer 332	01/03/2016	Crown Melbourne
Customer 333	27/12/2019	Crown Perth
Customer 334	01/03/2016	Crown Perth
Customer 335	04/07/2018	Crown Perth
Customer 336	22/06/2019	Crown Melbourne
Customer 337	01/03/2016	Crown Perth
Customer 338	01/03/2016	Crown Melbourne
Customer 339	01/03/2016	Crown Melbourne
Customer 340	01/03/2016	Crown Melbourne
Customer 341	01/03/2016	Crown Melbourne
Customer 342	05/12/2017	Crown Melbourne
Customer 343	01/03/2016	Crown Perth
Customer 344	01/03/2016 (Crown Melbourne) 21/03/2017 (Crown Perth)	Crown Melbourne and Crown Perth
Customer 345	01/03/2016	Crown Melbourne
Customer 346	09/02/2020	Crown Perth
Customer 347	02/03/2020	Crown Melbourne
Customer 348	20/04/2019	Crown Perth
Customer 349	21/05/2016	Crown Perth
Customer 350	26/06/2016	Crown Melbourne
Customer 351	01/03/2016	Crown Melbourne
Customer 352	01/03/2016	Crown Melbourne
Customer 353	15/09/2016	Crown Melbourne
Customer 354	31/01/2017	Crown Melbourne
Customer 355	01/03/2016	Crown Perth
Customer 356	2/07/2017	Crown Melbourne

Customer	Date DAB/SKA was opened ¹⁰¹	Crown Melbourne / Crown Perth
Customer 357	01/03/2016	Crown Perth
Customer 358	03/06/2019	Crown Melbourne
Customer 359	02/06/2019	Crown Melbourne
Customer 360	01/03/2016	Crown Melbourne
Customer 361	01/03/2016	Crown Perth
Customer 362	01/03/2016	Crown Perth
Customer 363	01/03/2016	Crown Melbourne
Customer 364	01/03/2016	Crown Perth
Customer 365	01/03/2016	Crown Perth
Customer 366	01/03/2016	Crown Melbourne
Customer 367	01/03/2016	Crown Melbourne
Customer 368	01/03/2016	Crown Melbourne
Customer 369	01/03/2016	Crown Melbourne
Customer 370	01/03/2016	Crown Perth
Customer 371	25/01/2019	Crown Melbourne
Customer 372	01/03/2016	Crown Melbourne
Customer 373	27/09/2019	Crown Perth
Customer 374	19/09/2019	Crown Melbourne
Customer 375	01/03/2016	Crown Melbourne
Customer 376	18/04/2019	Crown Melbourne
Customer 377	10/01/2020	Crown Melbourne
Customer 378	01/03/2016	Crown Melbourne
Customer 379	01/03/2016	Crown Melbourne
Customer 380	01/03/2016	Crown Melbourne
Customer 381	01/03/2016	Crown Melbourne
Customer 382	12/06/2018	Crown Melbourne
Customer 383	01/03/2016	Crown Perth
Customer 384	01/03/2016	Crown Melbourne
Customer 385	01/03/2016	Crown Melbourne
Customer 386	01/03/2016	Crown Melbourne
Customer 387	01/03/2016	Crown Melbourne

Customer	Date DAB/SKA was opened ¹⁰¹	Crown Melbourne / Crown Perth
Customer 388	02/05/2018	Crown Melbourne
Customer 389	01/03/2016	Crown Melbourne
Customer 390	01/03/2016	Crown Melbourne
Customer 391	01/03/2016	Crown Perth
Customer 392	01/03/2016	Crown Melbourne
Customer 393	22/01/2019	Crown Melbourne
Customer 394	01/03/2016	Crown Melbourne
Customer 395	29/06/2019	Crown Perth
Customer 396	04/10/2019	Crown Perth
Customer 397	27/08/2017 (Crown Melbourne) 29/03/2019 (Crown Perth)	Crown Melbourne and Crown Perth
Customer 398	01/03/2016	Crown Melbourne
Customer 399	03/07/2019	Crown Perth
Customer 400	21/08/2019	Crown Perth
Customer 401	25/12/2017	Crown Melbourne
Customer 402	01/03/2016	Crown Perth
Customer 403	01/03/2016	Crown Melbourne and Crown Perth
Customer 404	13/07/2017	Crown Perth
Customer 405	01/03/2016	Crown Melbourne
Customer 406	21/01/2019 (Crown Melbourne) 21/09/2018 (Crown Perth)	Crown Melbourne and Crown Perth
Customer 407	01/03/2016	Crown Melbourne
Customer 408	23/12/2019	Crown Melbourne
Customer 409	01/03/2016	Crown Melbourne
Customer 410	01/03/2016	Crown Melbourne
Customer 411	01/03/2016	Crown Melbourne
Customer 412	10/02/2017	Crown Melbourne
Customer 413	01/03/2016	Crown Melbourne
Customer 414	16/02/2020	Crown Melbourne
Customer 415	11/02/2020	Crown Melbourne

Customer	Date DAB/SKA was opened ¹⁰¹	Crown Melbourne / Crown Perth
Customer 416	31/10/2019	Crown Melbourne
Customer 417	12/07/2016	Crown Melbourne
Customer 418	29/06/2020	Crown Perth
Customer 419	01/03/2016	Crown Melbourne
Customer 420	19/06/2017	Crown Melbourne
Customer 421	01/03/2016	Crown Melbourne
Customer 422	01/03/2016	Crown Melbourne
Customer 423	01/03/2016	Crown Melbourne
Customer 424	06/02/2019	Crown Melbourne
Customer 425	01/03/2016	Crown Melbourne
Customer 426	18/07/2019	Crown Melbourne
Customer 427	01/03/2016	Crown Melbourne
Customer 428	01/03/2016	Crown Melbourne
Customer 429	01/03/2016	Crown Melbourne
Customer 430	01/03/2016	Crown Melbourne
Customer 431	01/03/2016	Crown Perth
Customer 432	01/03/2016	Crown Melbourne
Customer 433	05/06/2019	Crown Melbourne
Customer 434	01/03/2016	Crown Perth
Customer 435	01/03/2016 (Crown Melbourne) 30/04/2017 (Crown Perth)	Crown Melbourne and Crown Perth
Customer 436	11/10/2016	Crown Melbourne
Customer 437	01/03/2016	Crown Perth
Customer 438	01/03/2016	Crown Perth
Customer 439	8/07/2019	Crown Melbourne
Customer 440	01/03/2016	Crown Perth
Customer 441	8/03/2019	Crown Melbourne
Customer 442	01/03/2016	Crown Perth
Customer 443	01/03/2016	Crown Melbourne
Customer 444	09/08/2019	Crown Melbourne
Customer 445	31/08/2017	Crown Perth

Customer	Date DAB/SKA was opened ¹⁰¹	Crown Melbourne / Crown Perth
Customer 446	25/08/2016	Crown Melbourne
Customer 447	04/09/2018	Crown Melbourne
Customer 448	01/03/2016	Crown Melbourne
Customer 449	01/03/2016	Crown Melbourne
Customer 450	18/02/2019	Crown Melbourne
Customer 451	6/09/2019	Crown Melbourne
Customer 452	01/03/2016	Crown Melbourne
Customer 453	15/09/2017	Crown Perth
Customer 454	13/09/2019	Crown Melbourne
Customer 455	01/03/2016	Crown Melbourne
Customer 456	09/02/2019	Crown Melbourne
Customer 457	01/03/2016	Crown Perth
Customer 458	1/09/2017	Crown Melbourne
Customer 459	01/03/2016	Crown Melbourne
Customer 460	04/05/2016	Crown Melbourne
Customer 461	01/03/2016	Crown Melbourne
Customer 462	01/03/2016	Crown Melbourne
Customer 463	26/05/2017	Crown Melbourne
Customer 464	20/10/2019	Crown Melbourne
Customer 465	05/09/2019	Crown Melbourne
Customer 466	02/03/2019	Crown Perth
Customer 467	01/03/2016	Crown Melbourne
Customer 468	01/03/2016	Crown Melbourne
Customer 469	24/04/2017	Crown Melbourne
Customer 470	01/03/2016	Crown Melbourne
Customer 471	01/03/2016	Crown Perth
Customer 472	01/03/2016	Crown Perth
Customer 473	01/03/2016	Crown Melbourne
Customer 474	01/03/2017	Crown Perth
Customer 475	25/09/2018	Crown Perth
Customer 476	01/03/2016	Crown Melbourne

Customer	Date DAB/SKA was opened¹⁰¹	Crown Melbourne / Crown Perth
Customer 477	10/11/2016	Crown Melbourne
Customer 478	18/03/2017	Crown Melbourne
Customer 479	01/03/2016	Crown Melbourne
Customer 480	01/03/2016	Crown Melbourne
Customer 481	04/03/2016	Crown Melbourne
Customer 482	01/03/2016	Crown Melbourne
Customer 483	01/03/2016	Crown Melbourne
Customer 484	22/07/2017	Crown Melbourne
Customer 485	27/02/2020	Crown Melbourne
Customer 486	16/05/2016	Crown Melbourne
Customer 487	01/03/2016	Crown Melbourne
Customer 488	12/10/2019	Crown Perth
Customer 489	09/03/2019	Crown Melbourne
Customer 490	01/03/2016	Crown Melbourne
Customer 491	10/04/2019	Crown Melbourne
Customer 492	01/03/2016	Crown Melbourne
Customer 493	15/09/2016	Crown Perth
Customer 494	01/03/2016	Crown Melbourne
Customer 495	05/07/2016	Crown Melbourne
Customer 496	01/03/2016	Crown Melbourne
Customer 497	01/03/2016	Crown Melbourne
Customer 498	10/12/2016	Crown Perth
Customer 499	28/01/2020	Crown Melbourne
Customer 500	01/03/2016	Crown Melbourne
Customer 501	23/09/2017	Crown Perth
Customer 502	01/03/2016	Crown Melbourne
Customer 503	25/05/2017	Crown Melbourne
Customer 504	01/03/2016	Crown Perth
Customer 505	11/07/2017	Crown Melbourne