Royal Commission into Crown Melbourne

Schedule 2

No	Provision(s) of the AML/CTF Act/Rules which have or may have been breached	Details of acts or things which constitute breach or potential breach	Steps taken to remedy the breach or potential breach	Date of relevant conduct	Steps taken to ensure that the breach or potential breach will not be repeated
1	*Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (***AML/CTF Act***), sections 36, 81 and 82 *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument No.1 2007* (Cth) (***AML/CTF Rules***), Chapters 8 and 15	On 2 October 2020, AUSTRAC wrote to Crown Melbourne to inform it that its Regulatory Operations team: *'has identified potential non-compliance with the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (**AML/CTF Act**) and Anti-Money Laundering and Counter-Terrorism Financing Rules 2007 (**AML/CTF Rules**). This includes concerns with:* • *Ongoing Customer Due Diligence;* • *Adopting and maintaining an AML/CTF Program;* • *Compliance with Part A of an AML/CTF Program.'* These concerns were expressed as a result of a compliance assessment in September 2019 which focussed on Crown Melbourne's management of customers identified as high risk and as politically exposed persons (***PEPs***). These concerns have been referred to AUSTRAC's Enforcement Team, which has initiated a formal enforcement investigation	Crown Melbourne, Burswood Nominees Pty Ltd and Crown Sydney Gaming Pty Ltd formed a 'designated business group' (***DBG***) under the AML/CTF Act and adopted a joint anti-money laundering and counter-terrorism financing program (***Joint AML/CTF Program***) on 2 November 2020 which made a number of enhancements, including in relation to the assessment of risk, transaction monitoring and enhanced customer due diligence. Crown is in the process of embedding the new requirements in the Joint AML/CTF Program.	6 year period (October 2014 to October 2020)	In addition to the adoption and implementation of the new Joint AML/CTF Program, Crown is undertaking a program of change, led by the new Chief Compliance and Financial Crime Officer, Steven Blackburn. The steps Crown has taken and will take under Mr Blackburn's plan are summarised in Annexure 1.

Schedule 2

No	Provision(s) of the AML/CTF Act/Rules which have or may have been breached	Details of acts or things which constitute breach or potential breach	Steps taken to remedy the breach or potential breach	Date of relevant conduct	Steps taken to ensure that the breach or potential breach will not be repeated
		into the compliance of Crown Melbourne. As part of this investigation, Crown Melbourne has responded to a notice issued by AUSTRAC under section 167 of the AML/CTF Act. The period of AUSTRAC's enforcement investigation is 31 October 2014 to 16 October 2020 (***AUSTRAC Investigation Period***). Crown Melbourne considers that it may have breached: • the obligation in section 36 of the AML/CTF Act relating to the conducting of ongoing customer due diligence by not complying with all the requirements in Chapter 15 of the AML/CTF Rules; • section 81 of the AML/CTF Act, by not adopting and maintaining an AML/CTF Program that complied with all of the requirements set out in Chapters 8 and 15 of the AML/CTF Rules; and • section 82 by not complying with the requirements set out in its AML/CTF Program.			
2	AML/CTF Act, section 36	Failure to appropriately monitor deposits into bank accounts operated by Southbank Investments Pty Ltd (***Southbank***) with a view	Crown engaged: • Grant Thornton to undertake a forensic data analysis in relation	May 2013 to December 2019.	Southbank's bank accounts were closed in December 2019. Crown has liaised with

Schedule 2

No	Provision(s) of the AML/CTF Act/Rules which have or may have been breached	Details of acts or things which constitute breach or potential breach	Steps taken to remedy the breach or potential breach	Date of relevant conduct	Steps taken to ensure that the breach or potential breach will not be repeated
	AML/CTF Rules, Chapter 15	to identifying, mitigating and managing the risk that Crown Melbourne may reasonably face that the provision of a designated service at or through a permanent establishment of Crown Melbourne might (whether inadvertently or otherwise) involve or facilitate ML/TF.	to the Southbank account held with CBA over the period from August 2013 until December 2019 (when the account was closed), with a specific focus on identifying potential instances of structuring; and • Initialism, with the benefit of the forensic data analysis conducted by Grant Thornton, to assess whether there are indications of money laundering through the Southbank account. The results of these reviews were provided to Crown on 16 November 2020. Crown Melbourne has provided the Grant Thornton and Initialism reports to AUSTRAC and is assessing the transactions identified and considering whether any require the filing of a suspicious matter report (***SMR***) with AUSTRAC (to the extent an SMR has not already been filed).		ASIC in relation to its proposed deregistration of Southbank and has confirmed that it will take no steps to deregister Southbank without first consulting with ASIC, given that ASIC has informed Crown that Southbank is within the scope of ASIC's investigation. For detail of the further controls Crown has implemented in respect of the Southbank accounts, see row 5 of Annexure 1.
3	AML/CTF Act, sections 36, 81 and 82 AML/CTF Rules, Chapter 15	Crown commissioned a Junket Due Diligence and Persons of Interest Process Review which was completed by Deloitte in August 2020. It identified shortcomings in Crown's junket due diligence and persons of interest review processes. These shortcomings may constitute potential	Crown made a series of enhancements to its junket due diligence processes from mid-2017 onwards. These improvements were superseded by the decision in August 2020 by the Crown Resorts Board to temporarily suspend Crown Melbourne's dealings with junkets. This suspension was	At least 1 January 2010 to August 2020	See 'Steps taken to remedy the breach or potential breach' column.

Schedule 2

No	Provision(s) of the AML/CTF Act/Rules which have or may have been breached	Details of acts or things which constitute breach or potential breach	Steps taken to remedy the breach or potential breach	Date of relevant conduct	Steps taken to ensure that the breach or potential breach will not be repeated
		breaches of paragraphs 15.4 to 15.7 (relating to transaction monitoring) and 15.9 to 15.10 of the AML/CTF Rules (relating to enhanced customer due diligence) and, consequently, potential breaches of sections 36, 81 and 82 of the AML/CTF Act.	made permanent by the Crown Resorts Board on 17 November 2020.		
4	AML/CTF Act, section 36 AML/CTF Rules, Chapters 8 and 15	Crown Melbourne failed to identify the practice of 'aggregation' of transactions at the cage. Information which could be seen in the bank statements was lost in the process of data entry into the SYCO system. This resulted in transactions not being monitored as they should have been.	See response at rows 1 and 2 of this table. A direction was issued to relevant Crown staff in Melbourne on 12 November 2020, that under no circumstances should transactions be aggregated in Crown's casino management system. This direction was also incorporated into Crown Melbourne SOPs in October 2020.	2013 to September 2020	See response at rows 1 and 2 of this table
5	AML/CTF Act, section 41 AML/CTF Rules, Chapter 18	Potential non-compliance identified in relation to the completeness of data included in suspicious matter reports (***SMRs***), identified in an external review commenced, but not yet finalised, in relation to a sample of SMRs filed in November 2020.	Crown is considering the initial draft findings in the report.	November 2020	Crown will address any recommendations arising from this review once finalised (as per row 7 of Annexure 1)
6	AML/CTF Act, section 45 AML/CTF Rules, Chapter 17	Potential non-compliance in relation to the completeness of data included in international funds transfer instruction reports (***IFTIs***), identified in an external review commenced, but not yet finalised, in relation to a sample of IFTIs filed in March 2020.	Crown is considering the initial draft findings in the report.	March 2020	Crown will address any recommendations arising from this review once finalised (as per row 7 of Annexure 1)

Schedule 2

No	Provision(s) of the AML/CTF Act/Rules which have or may have been breached	Details of acts or things which constitute breach or potential breach	Steps taken to remedy the breach or potential breach	Date of relevant conduct	Steps taken to ensure that the breach or potential breach will not be repeated
7	AML/CTF Act, section 32	Crown identified one instance where Crown processed a threshold transaction report (*TTR*) with an expired ID.	Crown has placed a note on the customer's account to obtain updated ID when he is next at Crown.	January 2020	See 'Steps taken to remedy the breach or potential breach' column.
8	AML/CTF Act, section 43 AML/CTF Rules, Chapter 19	• 1 instance where Crown failed to obtain a residential address for a TTR from a customer. • 4 instances where an expired ID was provided by a customer at the time of conducting a TTR.	Crown Melbourne has included notifications on its Customer Management System to obtain the residential address of the relevant customer when they are next at the casino with a view to recalling the TTR from AUSTRAC and resubmitting it with the customer's residential address included.[1] In relation to the expired ID, in one instance Crown Melbourne obtained updated ID from the customer, and in the other three instances the AML team provided training to Table Games Management on this matter (where the issue originated). Table Games Management also communicated expressly on this issue with their staff. An improvement in reporting was noted following that training.	January 2019 to December 2019	Crown Melbourne addresses matters of non-compliance in the form of training 'Alerts' to the relevant Business Units (as it did in the case of the expired ID identified in the 'Steps taken to remedy the breach or potential breach' column).
9	AML/CTF Act, sections 123(1) and s123(3)	Prior to and during the ILGA Inquiry, Crown disclosed information, including SMR information, to its legal advisors at the time (Minter Ellison and counsel) in breach of	Promptly after having become aware of the breach, Crown applied to AUSTRAC for an exemption. On 17 November 2020 AUSTRAC granted Crown Resorts, Crown	At least 2019 to 17 November 2020	Exemption obtained from AUSTRAC.

[1] CRW.508.001.2986 (at .2990 - .2991), dated May 2019: Crown Melbourne Compliance Committee Agenda Item 4: AML/CTF Update.

Schedule 2

No	Provision(s) of the AML/CTF Act/Rules which have or may have been breached	Details of acts or things which constitute breach or potential breach	Steps taken to remedy the breach or potential breach	Date of relevant conduct	Steps taken to ensure that the breach or potential breach will not be repeated
		section 123(1) and 123(3) of the AML/CTF Act.	Melbourne, and Burswood Nominees (***Crown Entities***) an exemption (the *Anti-Money Laundering and Counter-Terrorism Financing (Exemption—Crown Entities) Instrument 2020 (No. 14))* (***Exemption Instrument***) which allows the Crown Entities to disclose SMR material to 'specified persons' in the Exemption Instrument (which includes its legal advisers and particular third party experts) in relation to specific 'matters' (which includes the ILGA Inquiry and this Victorian Royal Commission, amongst others).		
10	AML/CTF Act, section 123	On 29 July 2019, Crown disclosed information subject to the tipping off provisions in the AML/CTF Act to James Packer, in breach of section 123 of the AML/CTF Act.	On 21 October 2020, Crown announced the termination of the Controlling Shareholder Protocol dated 31 October 2018 which enabled the sharing of confidential information by Crown to Consolidated Press Holdings Pty Limited and James Packer.	29 July 2019	In accordance with row 9 of Annexure 1, revised AML/CTF risk awareness training has been released, which contains guidance around 'tipping off'. The Joint AML/CTF Program adopted in November 2020 also contains guidance on this obligation.
11	AML/CTF Act, section 45	Crown Melbourne did not report three IFTIs to AUSTRAC within 10 business days of the instruction (two from April 2018 and one from February 2019).	Upon being made aware of the issue by AUSTRAC, Crown Melbourne reported the IFTIs to AUSTRAC.	April 2018 to August 2019	The late-filed IFTIs were caused by a failure by the relevant members of the IT team to tag the IFTIs for filing with AUSTRAC. As a result of these issues, Crown Melbourne:

Schedule 2

No	Provision(s) of the AML/CTF Act/Rules which have or may have been breached	Details of acts or things which constitute breach or potential breach	Steps taken to remedy the breach or potential breach	Date of relevant conduct	Steps taken to ensure that the breach or potential breach will not be repeated
					• conducted a review of its IFTI reporting process, resulting in the implementation of a new workplace instruction relating to IFTIs and the transfer of the IFTI review and upload function from the IT team to the Crown AML team; • made changes to its process to remove the requirement that an IFTI be manually tagged for filing with AUSTRAC; and • included a weekly cross check conducted by the Crown AML team to ensure no IFTIs are inadvertently missed for filing with AUSTRAC.
12	AML/CTF Act, section 45	Crown Melbourne identified four errors in IFTIs reported to AUSTRAC in June 2018 and July 2018.	Crown Melbourne requested the IFTIs be returned to Crown by AUSTRAC, which occurred. Crown then resubmitted corrected IFTIs.	June and July 2018	N/A

Schedule 2

No	Provision(s) of the AML/CTF Act/Rules which have or may have been breached	Details of acts or things which constitute breach or potential breach	Steps taken to remedy the breach or potential breach	Date of relevant conduct	Steps taken to ensure that the breach or potential breach will not be repeated
13	AML/CTF Act, sections 32 and 45 AML/CTF Rules, Chapters 4 and 17	Implementation of a new Customer Management System called the Loyalty User Interface (***LUI***) in December 2016 impacted, or may have impacted, how Crown Melbourne meets its AML reporting requirements. Specifically it resulted in an increase in duplicate customer accounts, which increased the risk of incorrect Know Your Client (***KYC***) information being recorded and subsequently reported to AUSTRAC.	The identified issues were reported to IT with the AML and IT teams meeting on a regular basis to rectify the identified issues and propose solutions. In relation to the duplicate accounts, the AML team carried out regular checks on duplicate accounts and made amendments to correct the information. A project was also commenced to ensure each customer had one Crown identifier (regardless of which property the customer visited).	December 2016 to June 2019	No further action.
14	AML/CTF Act, section 32	Crown Melbourne identified some instances where a Card Play Extra ***(CPE***) account had been activated without the required ID on file. CPE functionality allows Crown Melbourne's customers to deposit or withdraw funds to a betting account.	Crown now identifies where a CPE account has been activated and does not have the required ID on file. Management is notified and the account is disabled.	Approximately September 2017 to November 2018	Crown also utilises the SPLUNK system to assist the Electronic Gaming Machines (***EGM***) team in its daily monitoring and checks for ID. Any daily non-compliance that is identified is then sent to the EGMs Area Managers / Operations Managers Remedial training is provided to those staff members who have failed to collect required ID, and a note is put against the file for the relevant staff member. Under the Joint AML/CTF Program (Part B) the list of

Schedule 2

No	Provision(s) of the AML/CTF Act/Rules which have or may have been breached	Details of acts or things which constitute breach or potential breach	Steps taken to remedy the breach or potential breach	Date of relevant conduct	Steps taken to ensure that the breach or potential breach will not be repeated
					Acceptable ID to join Crown Rewards has been limited to Primary Photographic identification. To have Card Play Extra enabled, a customer must be a Crown Rewards member.
15	AML/CTF Act, section 43 AML/CTF Rules, Chapter 19	In a sample of 10 TTRs filed with AUSTRAC, Crown Melbourne included a PO Box address in the 'residential address' field for the customer engaging in the threshold transaction. Under the AML/CTF Rules a PO Box cannot be used as a residential address. Crown Melbourne identified that this was occurring because for some customers, the PO Box and residential address had been entered in SYCO in the wrong order, leading to the wrong field being extracted for TTR filing.	Crown remediated the 10 TTRs and informed AUSTRAC of the steps it would take to ensure the issue did not reoccur.	April 2018 to May 2018	Crown implemented an automated check to detect and correct errors identified in its TTRs in advance of uploading the reports to AUSTRAC. Crown Melbourne also runs a quality assurance check over its TTRs to ensure data quality is maintained.
16	AML/CTF Act, section 123	Crown has recently become aware that in May 2018 an employee of Crown Melbourne may have 'tipped off' a customer in breach of section 123 of the AML/CTF Act following Crown Melbourne submitting a SMR. Crown is currently investigating the circumstances of this incident.	This incident is currently being investigated.	May 2018	In accordance with row 9 of Annexure 1, revised AML/CTF risk awareness training has been released, which contains guidance around 'tipping off'. The Joint AML/CTF Program adopted in November 2020 also contains guidance on this obligation.

Schedule 2

No	Provision(s) of the AML/CTF Act/Rules which have or may have been breached	Details of acts or things which constitute breach or potential breach	Steps taken to remedy the breach or potential breach	Date of relevant conduct	Steps taken to ensure that the breach or potential breach will not be repeated
17	AML/CTF Act, section 45 AML/CTF Rules, Chapter 17	On 17 April 2018 Crown identified that 55 IFTIs lodged during the period 20 March 2018 to 17 April 2018 contained errors in relation to the name of the customer due to an IT error and manual QA checks not being completed in accordance with policy.	Crown informed AUSTRAC of this issue on 19 April 2018 and manually reported the corrected IFTIs to AUSTRAC.	20 March 2018 to 17 April 2018	The change to the IT policy (see row 21 below) was reiterated to the AML team and IT, with specific meetings held on the topic. Additionally any IT change with an AML/CTF impact would be subject to enhanced testing and QA post-implementation
18	AML/CTF Act, sections 36, 43 and 45 AML/CTF Rules, Chapters 4, 15, 17, 18 and 19	For the 2018 calendar year, the following AML/CTF compliance breaches were identified (in addition to those referred to above): • 3 instances of TTRs processed without sufficient KYC information being collected; • 4 instances of TTRs being processed with inappropriate identification; • 1 instance of suspicious behaviour not raised as SMR; • 1 instance where a SMR raised was not reported through to the AML team;	While a number of the specific instances have been remediated, Crown is investigating the extent to which the remaining instances have been remediated.	January 2018 to December 2018	The Conduct and Counselling Policy was updated in November 2018 to address the seriousness of AML/CTF risk. In light of the non-compliance identified in 2018, the AML team reviewed its Alerting and Training program to determine if each could be supplemented to address the errors. Each breach is reported to the AML team with individual departments responsible for taking appropriate disciplinary action. If the incident is material or becomes a recurring issue with the particular staff

Schedule 2

No	Provision(s) of the AML/CTF Act/Rules which have or may have been breached	Details of acts or things which constitute breach or potential breach	Steps taken to remedy the breach or potential breach	Date of relevant conduct	Steps taken to ensure that the breach or potential breach will not be repeated
		• 8 instances of TTRs being completed without being correctly entered in the system for reporting; • 1 instance of a customer making an attempted TTR which then was split into two smaller transactions by staff and as such did not require reporting as a TTR; • 1 TTR was entered into in the system against an incorrect customer name; • 1 instance of an IFTI not flagged in SYCO for extraction, resulting in IFTI being reported 3 days late; • 6 instances of a failure to record a residential address; • 1 instance of an appropriate ID not being sighted; • 2 instances of an inappropriate ID being listed; • 6 instances of recording an expired ID; • 1 instance of an ID being accepted outside of Crown's approved listing; • 1 instance of an entry being incorrectly entered against the wrong customer number; and			members, serious disciplinary action is taken. Since February 2018, the Cash Transactions Reporting Manager sends a regular email to the business outlining errors that has been picked up in quality assurance testing of the TTR report, prior to its submission to AUSTRAC.

Schedule 2

No	Provision(s) of the AML/CTF Act/Rules which have or may have been breached	Details of acts or things which constitute breach or potential breach	Steps taken to remedy the breach or potential breach	Date of relevant conduct	Steps taken to ensure that the breach or potential breach will not be repeated
		• 1 instance of an invalid driver licence number being entered.			
19	AML/CTF Act, section 32	For the 2017 calendar year, the following AML/CTF compliance breaches were recorded: • 7 instances of a failure to record a residential address; • 1 instance of failure to record a date of birth; • 6 instances of recording an expired ID; • 2 instances of recording an ID that has no expiry date; • 1 instance of an appropriate ID not being sighted; and • 1 instance of an inappropriate ID being listed.	While a number of the specific instances have been remediated, Crown is investigating the extent to which the remaining instances have been remediated.	January 2017 to December 2017	
20	AML/CTF Act, sections 36 and 81	AUSTRAC made a number of findings on 26 June 2017 following a compliance assessment conducted in March 2017 into Crown's AML/CTF Program, policies and processes implemented to meet its obligations under the AML/CTF Act and AML/CTF Rules. The scope of the assessment included the following obligations under the AML/CTF Act:	Crown Melbourne made a range of improvements to its AML/CTF Program and associated procedures. The changes made are set out in letters to AUSTRAC dated 26 July 2017 and 26 October 2017, following further feedback received from AUSTRAC on 26 September 2017.	1 January 2016 to 18 May 2017	See 'Steps taken to remedy the breach or potential breach' column.

Schedule 2

No	Provision(s) of the AML/CTF Act/Rules which have or may have been breached	Details of acts or things which constitute breach or potential breach	Steps taken to remedy the breach or potential breach	Date of relevant conduct	Steps taken to ensure that the breach or potential breach will not be repeated
		• Section 84 – Standard anti-money laundering and counter-terrorism financing program; • Section 36 – Ongoing customer due diligence; • Section 41 – Reports of suspicious matters; • Section 42 – Reports of threshold transactions; and • Section 47 – AML/CTF compliance reports. AUSTRAC's findings, summarised below, were expressed by AUSTRAC as being 'some areas in which Crown Melbourne's AML/CTF Program could be amended to improve compliance with AML/CTF obligations'. Crown Melbourne considers the issues identified by AUSTRAC constitute potential non-compliance with the AML/CTF Act and the AML/CTF Rules. The findings included that: • Crown Melbourne's risk assessment would benefit from more consideration of how changes in the external ML/TF risk environment may affect the inherent and residual risk associated with the provision of	On 18 May 2018, AUSTRAC confirmed that it considered the compliance assessment closed.		

Schedule 2

No	Provision(s) of the AML/CTF Act/Rules which have or may have been breached	Details of acts or things which constitute breach or potential breach	Steps taken to remedy the breach or potential breach	Date of relevant conduct	Steps taken to ensure that the breach or potential breach will not be repeated
		its designated services and recommended that Crown: • review its risk assessment with a view to integrating ongoing assessment and consideration of changes in the external risk environment; • review its jurisdictional risk assessment and reassess the equal risk rating it accords all nations (except for Iran and North Korea); and • document its decision-making processes in relation to whether to maintain its business relationships with customers about whom it has adverse information. • Crown Melbourne's transaction monitoring program (***TMP***) appears to rely exclusively on the analysis of report output and recommended that Crown update its TMP to reflect the important role that behavioural observations of customers by			

Schedule 2

No	Provision(s) of the AML/CTF Act/Rules which have or may have been breached	Details of acts or things which constitute breach or potential breach	Steps taken to remedy the breach or potential breach	Date of relevant conduct	Steps taken to ensure that the breach or potential breach will not be repeated
		Crown staff can play in identifying suspicious activity. • KYC and Enhanced Customer Due Diligence (***ECDD***) were largely conflated in the AML/CTF Program and that Crown should update its KYC systems and controls, and distinguish them from its ECDD program. • Crown Melbourne should amend its AML/CTF Program so that its ECDD program mandates that a range of the measures set out in AML/CTF Rule 15.10(1) - (7) are undertaken every time that ECDD is triggered. • Crown Melbourne should amend its AML/CTF Program to include the procedures it follows in order to identify whether or not a customer is a PEP and who the beneficial owners of applicable customers are. • Crown Melbourne should amend its AML/CTF Program so that it is consistent on how Crown responds to discrepancies that arise in the course of verifying KYC information. • In relation to its employee training materials:			

Schedule 2

No	Provision(s) of the AML/CTF Act/Rules which have or may have been breached	Details of acts or things which constitute breach or potential breach	Steps taken to remedy the breach or potential breach	Date of relevant conduct	Steps taken to ensure that the breach or potential breach will not be repeated
		• in accordance with AML/CTF Rule 8.2.3, the purpose of staff awareness training should be captured in the AML/CTF Program; • the AML/CTF Program should be amended to provide more detail about the remedial training modules mentioned; and • the AML/CTF Program should be amended to provide more content in relation to how casino service can be used to facilitate ML/TF, and typologies of criminal misuse of casino services that do not relate to cash transactions. • Crown Melbourne should amend its AML/CTF Program to include appropriate systems and controls for Crown to determine whether any information in addition to the name, date of birth and/or residential address of a customer, should be verified at the time of onboarding the customer.			

Schedule 2

No	Provision(s) of the AML/CTF Act/Rules which have or may have been breached	Details of acts or things which constitute breach or potential breach	Steps taken to remedy the breach or potential breach	Date of relevant conduct	Steps taken to ensure that the breach or potential breach will not be repeated
		• Crown Melbourne should amend its AML/CTF Program to include the requirement to report changes in its enrolment details to AUSTRAC within 14 days of the change occurring.			
21	AML/CTF Act, section 45	In September 2017 Crown identified that due to an IT system error, it had not submitted 87 IFTIs between 26 June 2016 to 10 August 2017.	In August 2017 the 87 IFTIs were reported to AUSTRAC.	June 2016 to August 2017	Crown Melbourne engaged with AUSTRAC on the relevant steps, including moving the responsibility for lodging IFTIs to the AML team and implemented new processes and procedures to ensure that the risk of such errors is appropriately managed and controlled. The new processes and procedures included: • all IT jobs related to AML being listed on the AML Group Meeting Agenda for discussion and review; • the Chief Information Officer instructed his team that all AML IT related jobs must be

Schedule 2

No	Provision(s) of the AML/CTF Act/Rules which have or may have been breached	Details of acts or things which constitute breach or potential breach	Steps taken to remedy the breach or potential breach	Date of relevant conduct	Steps taken to ensure that the breach or potential breach will not be repeated
					attended to as top priority, with any issues identified escalated to him directly; • all issues which may have an AML/CTF impact on Crown's reporting obligations must be escalated to senior management; • retraining of relevant staff; and • procedures for a manual backup process to be created, for use where an automated system fails.
22	AML/CTF Act, sections 36 and 81	AUSTRAC made recommendations following a compliance assessment conducted during the period July 2016 to June 2017 into Crown's EGMs. The scope of the assessment included the following obligations under the AML/CTF Act: • AML/CTF Program; • TTRs; • OCDD; and	Crown agreed to implement the recommendations that AUSTRAC suggested in its letter. It said that it: • would update its Designated Services Risk Register and AUSTRAC Guidelines document (which it proposed to rename 'AML/CTF Guidelines'); • had commenced AML/CTF risk awareness training in respect of	1 July 2016 to 30 June 2017	

Schedule 2

No	Provision(s) of the AML/CTF Act/Rules which have or may have been breached	Details of acts or things which constitute breach or potential breach	Steps taken to remedy the breach or potential breach	Date of relevant conduct	Steps taken to ensure that the breach or potential breach will not be repeated
		• Record keeping. AUSTRAC made a number of recommendations summarised below. These were expressed by AUSTRAC as being 'some recommendations to strengthen Crown Melbourne's AML/CTF Program'. Crown Melbourne considers the issues identified by AUSTRAC constitute potential non-compliance with the AML/CTF Act and the AML/CTF Rules. The recommendations were to: • include the purchase of winning tickets or jackpots by third parties as a ML/TF risk factor in the ML/TF risk assessment and in Crown Melbourne's AUSTRAC Guidelines document; • include the purchase of winning tickets or jackpots by third parties as unusual or suspicious activity in risk awareness training for customer service attendants; • conduct regular refresher training for EGM customer service attendants on how to identify and report unusual or suspicious activity; • introduce additional automated monitoring rules to improve the	ML/TF risks related to gaming machines and Ticket in-Ticket Out (***TITO***) Tickets have commenced with relevant areas of the business; • had commenced providing dedicated training sessions to EGM customer service attendants (***CSAs***) on ML/TF risks related to the designated services provided by Crown Melbourne relevant to their position; • had reviewed its AML/CTF Risk Awareness Training framework by updating its online module 'Online Anti-Money Laundering' for additional examples of suspicious behaviour, including suspicious activity in relation to TITO Tickets; • had provided Alerts to the Cage, EGMs, Table Games, Security and Surveillance on key points to address in respect of potential suspicious activity; • had reiterated to CSAs in musters and briefings that if they see something, say something to the AML team, and/or through to management. CSAs were		

Schedule 2

No	Provision(s) of the AML/CTF Act/Rules which have or may have been breached	Details of acts or things which constitute breach or potential breach	Steps taken to remedy the breach or potential breach	Date of relevant conduct	Steps taken to ensure that the breach or potential breach will not be repeated
		identification of suspicious transactions or patterns of transactions; • conduct an independent review of the transaction monitoring program; • make records of investigations where no adverse findings were identified; • increase resourcing of the Compliance function; • reference the tipping off offence in the SMR reporting guidelines; • reference the requirement to verify customer's KYC information in the gaming payout procedures; and • reference the requirement to follow Crown Melbourne's AML/CTF Program and the obligations of the AML/CTF Act in the Conduct and Counselling guidelines.	reminded of the importance of their role in identifying potential unusual or suspicious activity and the prohibition against tipping off; • was investigating options available to it to automate appropriate elements of its TMP; • was proposing to adopt a Joint Program by 31 December 2018 and suggested it hold off on doing an independent review until that was in place; • had implemented a daily sign-off sheet for the team to make a record of matters reviewed, including where no adverse findings are identified and will be commissioning a new IT tool called 'CURA' to assist with recording; • was increasing the AML function including a new Group GM - AML, an AML Compliance Manager and an AML Officer; • had reviewed its Cage SOP to ensure the tipping off prohibition was adequately addressed and updated its AML/CTF risk		

Schedule 2

No	Provision(s) of the AML/CTF Act/Rules which have or may have been breached	Details of acts or things which constitute breach or potential breach	Steps taken to remedy the breach or potential breach	Date of relevant conduct	Steps taken to ensure that the breach or potential breach will not be repeated
			• awareness training and SMR form; and • updated its conduct and counselling guidelines. AUSTRAC responded on 19 June 2018 that it considered that Crown had taken action to address the ten recommendations and considered the assessment closed.		
23	AML/CTF Act, section 41 AML/CTF Rules, Chapter 18	On 25 August 2017, AUSTRAC provided feedback to Crown Melbourne on a review of a random sample of 50 SMRs lodged during the period 1 April 2016 to 1 March 2017. It identified the following areas as requiring attention and action: • the SMR 'grounds for suspicion' (*GFS*) field for several of the SMRs did not contain sufficient information about why Crown Melbourne found the activity suspicious; • although there was comprehensive quantitative data on customer activity in the SMRs, they lacked qualitative analysis of customer activity to indicate why Crown felt it was related to criminality; • 3 out of 50 of the SMRs did not include the name of the payee or payer associated with the transaction. Having this information	Crown met with AUSTRAC to discuss the findings on 29 August 2017. Crown also prepared an internal document evidencing its response to each of the findings. On 26 September 2017 AUSTRAC encouraged Crown Melbourne to submit a SMR when it observes unusually large cash transactions being processed over the cash desk in the Suncity Room, or any other suspicious activity. Crown responded on 26 October 2017 stating that it had reiterated to the staff (gaming and cage) working in the room and surveillance that the observation of the aforementioned unusually large cash transactions should result in the submission of a SMR.	1 April 2016 to 1 March 2017	Crown's revised AML/CTF Program sets out detailed processes to follow to ensure that all SMRs are filed in compliant form.

Schedule 2

No	Provision(s) of the AML/CTF Act/Rules which have or may have been breached	Details of acts or things which constitute breach or potential breach	Steps taken to remedy the breach or potential breach	Date of relevant conduct	Steps taken to ensure that the breach or potential breach will not be repeated
		is important as it enables analysts to follow funds between persons of interest; • 15 out of 50 of the SMRs reviewed did not include the industry or occupation of the customer; and • 20 out of 50 of the SMRs reviewed did not contain the details of transactions referred to in the GFS in the transaction component of the SMR form.			
24	AML/CTF Act, sections 36, 81 and 82 AML/CTF Rules, Chapters 8, 9 and 15	Crown did not have adequate controls to identify, mitigate and manage the ML/TF risk associated with the Suncity Room. For example, Crown accepts that: • the additional measures identified by Josh Preston in March 2020 should have been implemented at an earlier time. These measures included: • enhancements to supervision and surveillance in the Suncity Room, including, for example, an extra gaming inspector reporting regularly to the AML and Compliance team;	See steps in row 1 of this table. Specific controls implemented in relation to Suncity: • Cessation of Suncity's exclusive use of the VIP Room in Crown Melbourne in August 2019. • Prohibitions on cash transactions at the Suncity desk, and a requirement for all cash to be transacted at the Mahogany Room cash desk. • Imposition of a limit of $100,000 in cash held at the Suncity Room.	June 2014 to November 2020	See steps in row 1 of this table. Crown made a series of enhancements to its junket due diligence processes from mid-2017 onwards. These improvements were superseded by the decision in August 2020 by the Crown Resorts Board to temporarily suspend Crown Melbourne's dealings with junkets. This suspension was made

Schedule 2

No	Provision(s) of the AML/CTF Act/Rules which have or may have been breached	Details of acts or things which constitute breach or potential breach	Steps taken to remedy the breach or potential breach	Date of relevant conduct	Steps taken to ensure that the breach or potential breach will not be repeated
		• enhancements to SMR reporting relating to the Chau Junket and the Suncity Room as a result of the enhanced level of information received from any report or observation from the extra gaming inspector; and • additional restrictions on cash deposits for the Chau Junket and junket representatives and in connection with the Suncity Room; • Crown should not have permitted a cash desk at which a junket player or representative could buy-in or provide cash in exchange for commission chips within the Suncity Room; and • the Suncity cash desk transactions should have been subject to further investigation by the AML team to determine whether they were suspicious.	• Implementation of an additional control in the Suncity Room that Suncity staff can only take clear plastic bags into the room to allow Crown Surveillance to observe the contents of the bags.		permanent by the Crown Resorts Board on 17 November 2020.

Schedule 2

Annexure 1 – Relevant aspects of AML/CTF change program / Junkets/POI/Significant player review

No	Area	Changes already made	Proposed next steps
AML/CTF Change Program			

1.	**Financial Crime Resourcing and Team Structure**	• An expanded and better resourced Compliance and Financial Crime department independent of business units has been created with direct reporting lines to the Board.
		• Steve Blackburn commenced as the Chief Compliance and Financial Crime Officer on 1 March 2021.
		• Nick Stokes, Head of Financial Crime and Group Money Laundering Officer, was appointed as AML/CTF Compliance Officer for each of the Crown reporting entities on 2 November 2020.
		• Further new Financial Crime roles have been created and appointed:
		  • Group Senior Manager Financial Crime – Customer Investigations (commenced 21 October 2020);
		  • Financial Crime Investigations Officer Melbourne (commenced 19 October 2020);
		  • Group Senior Analyst Financial Crime – Customer Investigations (commenced 21 December 2020);
		  • Group Financial Crime Manager – Data Analytics (commenced 21 December 2020);
		  • Financial Crime Manager Sydney (commenced 14 December 2020);
		  • 2x Group Financial Crime Analysts (commenced 4 January 2021);
		  • Financial Crime Manager Perth (commenced 18 January 2021);
		  • Group Senior Manager Financial Crime – Customer Intelligence and Due Diligence (commenced 11 January 2021); and
		  • Financial Crime Investigations Officer Sydney (commenced 1 March 2021).
			• Recruitment of the following additional positions is underway:
			  • Group Financial Crime Analyst (three positions);
			  • Group Senior Manager Financial Crime - Assurance & Testing;
			  • Perth and Sydney Financial Crime Analysts; and
			  • Financial Crime Project Manager (contractor).
			• Additionally, Mr Blackburn is currently assessing the Financial Crime team's structure. He has the support of the Chair and the Crown Board to increase the current resourcing levels (refer to item 13 below).

2.	**ML/TF Risk Assessment**	• Promontory was engaged in September 2020 to provide Crown with an assessment of potential financial crime vulnerabilities in its business, and a forward-looking strategic assessment of capabilities to manage the risks associated with financial crime. Promontory	• Informed by the results of Promontory's financial crime vulnerability assessment,

Schedule 2

No	Area	Changes already made	Proposed next steps
		have presented their preliminary findings to Crown's Financial Crime team and Crown expects to receive their draft report shortly.	Crown will conduct an enterprise-wide ML/TF risk assessment. • Refer also to item 13 below.

3.	**AML / CTF Program**	• As part of Crown's ongoing roll-out of the AML/CTF Change Program, a Joint AML/CTF Program (comprising the AML/CTF Part A Program, which includes the AML/CTF Policies and Procedures, and Part B Program) (***Joint AML/CTF Program***) was endorsed by the Crown Resorts Board for adoption by each of Crown's reporting entities. Part A was approved by the boards of each of the reporting entities, being Crown Sydney, Crown Melbourne and Crown Perth, on 2 November 2020.
		• Among other things, Part A of the new Joint AML/CTF Program provides for greater Board and senior management oversight and responsibility for driving a positive culture of AML/CTF compliance (see item 4 below for more information).
		• Under the Joint AML/CTF Program, the AML/CTF Compliance Officer has responsibility for the continued compliance of each of the reporting entities with the requirements of the AML/CTF Act and the AML/CTF Rules, as well as the Joint AML/CTF Program. Under sections 7.1 and 19 of the Part A Program the AML/CTF Compliance Officer has a direct reporting line to the Crown Resorts Board and both an opportunity and requirement to raise significant AML/CTF matters.
		• The Joint AML/CTF Program also includes a revised transaction monitoring program (***TMP***). This includes the introduction of an automated TMP through Sentinel and manual transaction monitoring.
		  • Sentinel is discussed further in item 6 below.
		  • As part of the manual aspect of the TMP, Crown has implemented an internal process for the generation of Unusual Activity Reports (***UARs***), which are submitted internally for review by the Financial Crime team pursuant to the AML/CTF Policies and Procedures. The Financial Crime team then decides whether to file a suspicious matter report (***SMR***) with AUSTRAC and/or to conduct enhanced customer due diligence.
		• The relevant business stakeholders approved and endorsed the Business Unit Standard Operating Procedures to give effect to the new Joint AML/CTF Program.
			• Continuing embedment of the Joint AML/CTF Program with oversight and guidance from Mr Blackburn.
			• Refer also to item 13 below.
			• Crown is preparing a further direction to the Significant Cash Policy to lower the cash deposit thresholds at the cage for Crown Melbourne and Crown Sydney, as follows:
			  • from $50,000 to $25,000 for cash deposits at the cage that require a Source of funds declaration; and
			  • from $150,000 to $100,000 for cash deposits at the cage requiring a source of funds declaration and approval from the COO (or equivalent) or the CFO Australian Resorts and either the Group AML Compliance Officer or the Group GM Risk & Audit is required.

Schedule 2

No	Area	Changes already made	Proposed next steps

		• Crown has also adopted a number of specific policies and procedures aimed at mitigating further its exposure to money laundering risk, including:
		  • On 1 October 2020 Crown communicated to its staff that it would no longer permit junkets or other customers to utilise money remitters. On 21 October 2020, Crown notified its staff that it would no longer authorise third party transfers without the written approval of the COO (or equivalent) or the Group General Manager, AML. On 16 November 2020 Crown introduced the formal Third Party Transfers and Remitters Policy which articulates this.
		  • On 16 November 2020 Crown issued a Significant Cash Policy direction from the Chief Executive Officer, which prohibited:
		  • cash deposits at the cage over $250,000;
		  • cash deposits at the cage over $200,000 unless a source of funds declaration was provided by the patron depositing the cash and written approval was provided from the respective property COO (or equivalent) or the CFO Australian Resorts and either the Group AML/CTF Compliance Officer or the Group GM Risk & Audit (or equivalent); and
		  • cash deposits at the cage over $100,000 unless a source of funds declaration was provided by the patron depositing the cash and approval was given by the Cage Supervisor for the deposit.
		  • On 5 December 2020, Crown issued a Corporate Policy Statement on Source of Funds for cash transactions at the cage or a gaming location. The Policy was revised on 22 February 2021, and now provides that if a customer reaches the following cash deposit limits on a calendar day at the cage or a gaming location, the following specific actions must be taken:
		  • all cash transactions of $10,000 or more require a TTR. A UAR form may be completed and sent to the AML team if the staff member deems it appropriate;
		  • for cash deposited during a calendar day in the amount of $50,000 - $149,999, a source of funds declaration must be completed by the patron	

Schedule 2

No	Area	Changes already made	Proposed next steps
		and approved by the Cage Supervisor or Table Games Manager. A UAR must also be completed and sent to the AML team; • for cash presented for a calendar day between $150,000 and $200,000, a source of funds declaration must be completed by the patron and approved by the respective property COO, CFO (or designee) and either Group AML/CTF Compliance Officer or Group GM Risk and Audit Manager (or designee). A UAR must be completed and forwarded to the AML team; • cash amounts of $200,000 or more are prohibited and will not be accepted in any circumstances (which includes accumulated transactions in a calendar day); and • single cash buy ins for $100,000 (revised to $50,000 on 10 March 2021 in Melbourne and to $20,000 in Perth) or more at a table, must be referred to the cage and a source of funds declaration must be completed by the patron and approved by the Cage Supervisor or Table Games Manager. A UAR must also be completed and sent to the AML team. These are in addition to specific controls adopted in relation to Crown's bank accounts, which are summarised in item 5 below. • On 18 February 2021, the $250,000 threshold in the Significant Cash Deposit Policy direction was reduced to $200,000, the $200,000 threshold was reduced to $150,000 and the $100,000 threshold was reduced at Crown Melbourne (and Crown Sydney, to the extent it is permitted to operate a casino licence) to $50,000 and to $20,000 for Crown Perth. For this lower threshold the Policy was also amended so that a Cage Supervisor or above can approve the deposit provided the patron provides a source of funds declaration.	
4.	**AML reporting structures and governance**	• The Joint AML/CTF Program creates a prescriptive framework for both formal reporting and informal escalation of AML/CTF related matters. It provides for Crown Board oversight of AML/CTF matters and requires quarterly reporting to the Crown Board and monthly reporting to Crown senior management and that material AML/CTF matters be escalated at each Crown Board meeting or as frequently as required.	• Refer to item 13 below. • The Sydney ERCC is in development and will be formed with the commencement of gaming at Crown Sydney.

Schedule 2

No	Area	Changes already made	Proposed next steps

		• The AML/CTF Policies and Procedures provide that the Board and senior management of both Crown Resorts and each reporting entity are the owners of ML/TF risk. Pursuant to s 7.5 of the Part A Program significant AML/CTF matters will also be raised with a newly established AML/CTF Committee which in turn will report matters to the Executive Risk and Compliance Committees (***ERCC***) of each Crown reporting entity.
		• The Group AML/CTF Committee meets quarterly and comprises representatives from each of the relevant business units of each Crown entity. The Group AML/CTF Committee met in January 2020, November 2020 and January 2021. The Group AML/CTF Committee did not meet as scheduled in 2020 due to the closure of Crown's properties as a result of the COVID-19 pandemic. The remaining scheduled meeting dates for 2021 are as follows: 29 April 2021, 15 July 2021 and 28 October 2021.
		• The Crown Financial Crime team has also provided updates to the ERCCs in Melbourne and Perth as follows:
		  • in November 2020 and January 2021 in Melbourne; and
		  • in November 2020 and February 2021 in Perth.
		• The agenda for the Melbourne ERCC, as well as the Perth ERCC includes a standing AML/CTF agenda item.
		• The agenda for the Crown Resorts Board includes a standing AML/CTF agenda item. Detailed AML/CTF updates were provided to the Crown Resorts Board in November 2020 and February 2021.
		• The agenda for the Crown Resorts Risk Management Committee includes a standing AML/CTF agenda item.	

5.	**Riverbank / Southbank and enhanced Patron Account Controls**	• The Riverbank and Southbank bank accounts were closed in December 2019. Since that time, neither Riverbank nor Southbank has operated a bank account. • The only patron accounts for Crown Sydney are onshore bank accounts in the name of Crown Sydney Gaming. • A direction was issued to relevant Crown staff in Perth on 24 September 2020, and in Melbourne on 12 November 2020, that under no circumstances should transactions be aggregated in Crown's casino management system. This direction was also incorporated into Crown Melbourne and Crown Perth SOPs in October 2020. Additional controls have	• Crown is undertaking a 'lookback' of the transactions identified in the reviews of the Riverbank and Southbank accounts undertaken by Grant Thornton and Initialism to identify whether there is any further reporting to AUSTRAC required. • There are challenges in eliminating cash deposits by patrons at ANZ branches.

Schedule 2

No	Area	Changes already made	Proposed next steps

		been implemented over Crown's patron bank accounts to mitigate the risk of criminal exploitation (the ***Patron Account Controls***), including:
		• On 8 April 2020, an Executive Office Memorandum was circulated to relevant Crown employees informing them that Crown will no longer make or receive payments to or from third parties without prior written approval from the property CEO or equivalent and the AML/CTF Compliance Officer. This direction was further memorialised in another Executive Office Memorandum on 31 July 2020 with further instructions on the ban on all third party transfers and a Q&A for staff on what they are to do if a customer approaches Crown requesting to transfer funds to a third party, or requesting that a third-party be able to transfer funds to Crown.
		• On 16 November 2020 (pursuant to cl 7.5(i) of the Part A Program and cl 6.2.3 of the AML/CTF Policies and Procedures) Crown introduced a manual rule for bank statement monitoring, which requires bank statements be monitored weekly and cash deposits reviewed to identify suspicious transactions.
		• On 16 November 2020, Crown adopted the Third Party Transfers and Money Remitters Policy (the ***Third Party Policy***). The Third Party Policy notes that Crown:
		  • does not accept payments from third parties (including money remitters) into its accounts for the benefit of a Crown customer; and
		  • will not make payments to third parties (including money remitters) on behalf of a Crown customer.
		The Third Party Policy prescribes a detailed procedure to be followed if a departure from the default position of not accepting payments from third parties is to be approved.
		• On 4 January 2021, Crown implemented the Return of Funds Policy, which states that Crown will:
		  • only accept payments that are transferred into its bank account from personal bank accounts belonging to the patron seeking to transfer funds to Crown;
			Crown and ANZ are discussing the implementation of a reporting mechanism which would enable Crown Resorts to be notified when there is a potential customer cash deposit into a Crown Resorts bank account. In particular, Crown is engaging with ANZ to obtain direct electronic daily feeds of its bank statements in order to automate and facilitate the process of identifying anomalies.
			• Refer also to item 12 below.

Schedule 2

No	Area	Changes already made	Proposed next steps
		• return all of the following types of payments: (a) cash deposits; (b) funds transferred from a company or trust bank account (unless approved); (c) funds transferred by a third party for the benefit of a Crown patron account (unless approved); (d) funds transferred when the description or narration is misleading as to purpose; and (e) funds transferred where the patron has not provided a receipt or supporting documentation.	
6.	**Transaction Monitoring Program / Sentinel**	• Crown's new Joint AML/CTF Program includes a revised transaction monitoring program (***TMP***). • Crown has rolled out an automated TMP through Sentinel. Sentinel has two features: (i) it automatically monitors and alerts for transactions (the ***Rules Feature***) and (ii) allows Crown to view a 'Customer Intelligence' dashboard which provides a summary of the customer's profile and their gaming and transaction activity. • The Rules Feature is a risk-based TMP which contains rules designed to detect unusual transactions, patterns of transactions or behaviours, including transactions on accounts which are not consistent with rated play. Although the Rules Feature is currently live with a large number of standalone transaction monitoring rules in operation, other transaction monitoring rules are still being calibrated. Further aspects of the risk-based Rules Feature in Sentinel are also being developed. • On 3 February 2021 the Financial Crime Team for Crown Melbourne and Crown Perth commenced monitoring and dispositioning of Sentinel alerts in the Rules Feature. There are currently 15 Sentinel rules, which cover two key risk areas, being cash transactions and high risk alerts. The alerts are automated in Sentinel, but the dispositioning and triage process is manual. Crown is working towards this becoming a digitised process.	• Continued rollout of Crown's automated transaction monitoring program with oversight and guidance of Mr Blackburn. • Initialism has been engaged to conduct a transaction monitoring source information review. This is a review of Crown's transaction monitoring program focusing on the source data being ingested into the TMP from the various Crown systems, a review of the TMP testing documentation, the appropriateness of the 15 Sentinel rules, and whether the 2019 Initialism TMP recommendations have been implemented. Initialism are due to provide their findings by Friday 19 March. Crown will address Initialism's recommendations for improvements to Crown's TMP process.

Schedule 2

No	Area	Changes already made	Proposed next steps

7.	**Regulatory Reporting (IFTIs/ SMR/ UARs and TTRs)**	• As noted above at item 3, Crown has developed a new UAR process as a way to systematise internal reporting of unusual activity for a determination by the Financial Crime team as to whether a SMR should be filed with AUSTRAC.
		• The current UAR process is manual. On 25 February 2021 the Financial Crime Team commenced a pilot of the digitised UAR process. While the digitised system will still be subject to a range of future enhancements, the following components are currently functional:
		  • UAR form;
		  • UAR review and triage fields;
		  • Investigation report; and
		  • SMR decisioning fields.
			• Crown has initiated external reviews of its international funds transfer instruction reports (***IFTI***), SMR, and threshold transaction reports (***TTR***) reporting processes to ensure it is complying with the requirements of Chapters 17, 18 and 19 of the AML/CTF Rules when submitting these reports. Crown will address any recommendations arising from those reviews.
			• Crown has also set up a test reporting account with AUSTRAC for Crown Sydney to test the bulk upload process for TTR and IFTI files is working. Further testing of this account is planned with AUSTRAC.

8.	**ECDD / KYC**	• Enhanced customer due diligence process has been adopted in Crown's AML/CTF Policies and Procedures (as part of the new Joint AML/CTF Program). The AML/CTF Policies and Procedures provide for a process in clause 3 regarding customer risk assessments, and how those customers who are high or critical risk are to be escalated. • On 12 November 2020 Crown also introduced its Escalation of Critical Risk Customer Policy, which requires specific matters to be addressed to determine whether a critical risk customer should be retained; Crown has also introduced a new Persons of Interest (***POI***) Group Committee. This became active on 14 October 2020, with a decisioning tool developed and in operation (see items 14 – 17 below for further details on further patron specific controls implemented by Crown.)	• Crown will review its Escalation of Critical Risk Customer Policy to address comments made in the Bergin Report as to the definition of critical risk customers and the process for considering whether they should be retained.

9.	**AML/CTF Training**	• Revised online "Awareness" training module has been released. As at 28 February 2021:
		  • 11,470 Crown employees (88%) have completed the AML/CTF Awareness Training;
		  • 2,695 Crown Melbourne Contractors have also completed the training.
			• Crown will conduct refresher AML/CTF training for moderate and high risk employees and contractors on an annual basis.

Schedule 2

No	Area	Changes already made	Proposed next steps

		• "BU Specific" targeted face-to-face training for Table Games (including VIP International), Gaming Machines, Cage, Security & Surveillance, Hotels and Food and Beverage, is being delivered (typically to supervisors and above, noting a number of Table Games staff have currently been stood down due COVID-19 restrictions). As at 9 March 2021:
		  ◦ 909 employees (92%) at Crown Perth;
		  ◦ 1,258 (77%) at Crown Melbourne;
		  ◦ 183 employees (100%) at Crown Sydney.
		  ◦ 102 (86%) of the Business Operations Teams (***BOT***) (senior management) at all properties have also received targeted training. 100% of the Sydney BOT have attended training, and at least 83% of the BOT in Melbourne and Perth have completed training. Those who have missed the training in Melbourne and Perth will have an alternative session arranged.
		• 100% of C-suite executives have also received face-to-face AML/CTF training.
		• A new face-to-face AML/CTF training module was delivered to the Boards and senior management of Crown Resorts, Crown Sydney, Crown Melbourne and Crown Perth on 8 March 2021.
			• AML training scheduled for late March will cover the roll out of a new digitised UAR and SMR workflow for staff in the Crown Table Games, Gaming Machines and Cage business units. The information sessions will provide relevant Crown employees in the casinos and the cage with an understanding of the UAR and SMR process and how to identify and escalate unusual activity through the new system and workflow.
			• A training calendar is also being prepared. The topics for the training will change depending on relevant trends identified in the business, changes to policy or industry guidance. Business units will also receive further AML training.
			• Face-to-face AML/CTF training for board and C-suite executives will be reconducted annually and each new board member and c-suite executive will receive face-to-face AML/CTF training within one month of commencing their role.

10.	**Employee Due Diligence**	• In accordance with s9 of its Part A Program and s4 of the AML/CTF Policies and Procedures, Crown has allocated all internal Crown roles an AML risk category for the purposes of conducting Employee Due Diligence screening:
		  ◦ On 20 October 2020, Crown undertook an initial screen of 6,100 employees.
		  ◦ During December 2020 all 'moderate' and 'high risk' employees were uploaded to Dow Jones for screening. This was updated again on 26 January 2021.
			• Automation of the upload process for all moderate and high risk employees is being developed by the IT Department to ensure any new employees are subject to screening.
			• Further enhancement of the Employee Due Diligence Framework (including additional checks) at onboarding or if

Schedule 2

No	Area	Changes already made	Proposed next steps
			transferred to a higher risk role, are being considered.

11.	**Independent review of the Joint AML/CTF Program**		• In the fourth quarter of 2021, Crown will engage a third party consultancy firm to conduct an independent review of the Joint AML/CTF Program.. The review will assess:
			  ◦ the effectiveness of the Joint AML/CTF Program having regard to the ML/TF risk of each reporting entity in the designated business group;
			  ◦ whether the Joint AML/CTF Program complies with the AML/CTF Rules;
			  ◦ whether the Joint AML/CTF Program has been effectively implemented; and
			  ◦ whether each reporting entity in the designated business group has complied with the Joint AML/CTF Program.
			• Crown will undertake to have a further independent review conducted twelve months after the independent review.

12.	**Deloitte Forensic Review**	• Deloitte have been engaged by Crown to conduct a forensic review and controls assessment to address the recommendations in the Bergin report. The review commenced on 22 February 2021 and consists of the following three phases of work: ◦ **Phase 1** will assess the design and operating effectiveness of Crown's current Patron Account Controls. This phase will be completed sooner than Phases 2 and 3 to ensure the Crown Resorts Board and ILGA are provided with comfort as soon	• Crown anticipates that Phase 1 of Deloitte's review will be completed on or before the end of March 2021. . • The timing for Phases 2 and 3 of Deloitte's review will be determined in early April.

Schedule 2

No	Area	Changes already made	Proposed next steps

		as possible that Crown has appropriately mitigated the risk of transactions occurring through Crown's current patron accounts that are similar to those identified in the Grant Thornton and Initialism Reports in relation to the Riverbank and Southbank accounts dated November 2020.
		• **Phase 2** will confirm whether there are any transactional patterns or behaviours indicative of any money laundering typologies through historic or current Crown patron accounts, including but not limited to the typologies identified in the Grant Thornton and Initialism Reports. This phase will provide the Crown Resorts Board and ILGA with full visibility as to:
		  • whether there were other transactional patterns or behaviours indicative of money laundering through the Riverbank or Southbank accounts not identified in the Grant Thornton and Initialism Reports; and
		  • the extent to which any other Crown patron accounts (including all historic patron accounts) may also have been infiltrated by criminal elements.
		Further, Deloitte will undertake a sample review of other Australian or overseas bank accounts held by Crown or other legal entities associated with Crown's Australian casino operations. If it identifies any accounts that were used, or capable of being used, as patron accounts it will add these to the scope of the Phase 2 review.
		• **Phase 3** will provide comfort to the Crown Resorts Board and ILGA as to whether Crown's broader control framework appropriately mitigates the risk of any transactions similar to those identified in Phase 2 continuing to occur through the Crown's current patron accounts.	

13.	**Steven Blackburn proposals**	• Mr Blackburn's plan is to continue the process of embedment of Crown's new Joint AML/CTF Program, including the roll out of Crown's automated transaction monitoring system, Sentinel. In parallel, Crown will conduct an enterprise-wide ML/TF risk assessment, informed by the results of an ML/TF vulnerability assessment that the external risk management consultancy, Promontory, is due to complete into Crown's vulnerability to criminal exploitation.	• Informed by Promontory's work, the findings of the Inquiry and his assessment of the Joint AML/CTF Program, Mr Blackburn will table with the Board a detailed report that sets out his assessment of Crown's current maturity across all elements of financial crime risk management and his plan as to:

Schedule 2

No	Area	Changes already made	Proposed next steps
			• the Financial Crime team's structure, resourcing and capabilities; • financial crime governance and oversight; • additional controls that may be necessary or desirable to address financial crime risks in the casinos' operations; and • further steps that may be necessary or desirable to build and embed a positive culture of financial crime risk awareness and compliance. • This report will be presented to the Board on or before 31 May 2021.
Junkets/POI/Significant player review			
14.	**Cessation of dealing with junket operators**	• On 17 November 2020, the Crown Board determined that Crown will permanently cease dealing with all junket operators, subject to consultation with gaming regulators in Victoria, Western Australia and New South Wales. Crown informed all recently active junket operators of this decision by early December 2020.	• Complete. • Should it be required, Crown is willing to provide the Authority with an undertaking in a form suitable to the Authority to the effect that Crown will not deal with junket operators in the future without regulatory approval.
15.	**POI review**	• In April 2020, Crown commissioned Deloitte to undertake a review of its junket due diligence and POI process. The final report was received from Deloitte in August 2020. • The Crown Resorts Board resolved to adopt the recommendations on 18 August 2020. • A workplan to implement the Deloitte recommendations was endorsed by the Board on 10 September 2020.	• Complete

Schedule 2

No	Area	Changes already made	Proposed next steps
		• Recommendations in relation to customer due diligence have been implemented, including expansion of the POI Committee to a group-wide committee, implementation of a POI Decision Assessment tool, and providing the Crown Melbourne Compliance Committee and the Crown Resorts Board Risk Management Committee with oversight of POI process.	

16.	**Significant Player Review**	• A new process was implemented in 2020 (and subsequently further refined) to assist with customer due diligence and identification of individuals with whom Crown should cease dealing.
		• A Significant Player Review Policy (***SPR Policy***) to support the process is in development.
		• The Significant Player Review involves a review (on an ongoing basis) of top-end local and domestic players (determined by certain theoretical or actual revenue spend thresholds during defined periods) across all three of Crown's properties to determine whether (i) to continue to deal with the patron; (ii) further investigation is required; or (iii) cease to do business with the patron. The review also assesses players based overseas who play Gaming Machines.
		• Reviews have been undertaken across all three of Crown's Australian properties: The SPR Policy outlines a framework for completing further Know Your Customer (***KYC***) in accordance with the AML/CTF Rules on customers who trigger certain theoretical or actual revenue spend thresholds at Crown during defined periods:
		  • Reviews completed for in excess of 1,250 top customers in Melbourne and in excess of 500 Sydney based customers who are expected to become Crown Sydney customers. Of the customers referred to the POI Committee, 90 have been issued with a Withdrawal of Licence (***WOL***) either at the meeting or subsequently for failure to provide sufficient source of wealth information. A further 93 customers are awaiting decision by the POI Committee.
		  • Perth's review of its top customers continues with in excess of 250 customers currently subject to reviews.
		  • As part of the top locals review, a new workstream for approximately 54 formerly international customers now domiciled in Melbourne has been initiated. Of the patrons reviewed, 16 have now been approved to continue as customers, and 6 have been issued with a WOL.
			• Finalisation of SPR Policy.
			• Reviews will be undertaken on an ongoing basis as new customers reach certain trigger thresholds and as periodic re-assessments are undertaken.

Schedule 2

No	Area	Changes already made	Proposed next steps
17.	**Credit approval process**	• The credit decision making process has been separated from the Premium Player due diligence and approval process.	• Complete.
18.	**Information sharing protocols with relevant law enforcement agencies**	• Nick Kaldas engaged to assist with developing information sharing protocols with law enforcement agencies. • A Memorandum of Understanding (***MoU***) has been discussed with the Australian Crime and Intelligence Commission (***ACIC***). However, implementation of the MoU is currently on hold pending resolution of various regulatory matters. • MoUs are also being pursued with the police forces in NSW, Victoria and Western Australia.	• Continued engagement with relevant law enforcement agencies for the development and implementation of information sharing arrangements.