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, 45 and potentially others. *Casino Control Act 1991* (Cth), section 68.	A surveillance log entry (***SLE***) dated 17 March 2021 records that on 16 March 2021 an employee made 'remarks relating to money laundering and Crown staff being aware and assisting in money laundering activities with patrons'. A copy of the SLE is at **Annexure 1**. From initial inquiries, Crown understands that one of the matters referred to in the SLE relates to a service offered by Crown between approximately 2013 and 2016 by which internationally domiciled patrons staying at a Crown hotel could use debit or credit cards (including China UnionPay cards) to obtain a receipt from the Crown hotel that could be presented at the cage, where it was able to be redeemed for chips or for a deposit to the patron's account.	The Board of Crown Resorts Limited has recently commenced its own urgent investigation of each issue raised in the SLE and further steps to be taken will depend upon the results of that investigation. Crown will continue to update the Commission with findings as this investigation develops.	To be confirmed, but approximately 2013 – 2016.	N/A
1. KYC / customer identification					
2	AML/CTF Act, section 32 *Anti-Money Laundering and Counter-Terrorism Financing Rules*	During the 2010 calendar year, Crown recorded the following breaches by its employees in respect of Crown's customer identification procedures: • 10 instances of a failure to record a residential address;	While a number of the specific instances have been remediated, due to the passage of time Crown is not able to determine whether every instance was remediated.	January 2010 – November 2010	Crown's practice is that 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.

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
	Instrument 2007 (No. 1) (Cth) (***AML/CTF Rules***), Chapter 4	• 4 instances of recording an expired ID; • 8 instances of an appropriate ID not being sighted; and • 4 instances of an appropriate ID being sighted, but not being entered into Crown's internal records system..			At times Crown Melbourne may address matters of non-compliance in the form of training 'Alerts' to the relevant Business Units.
3	AML/CTF Act, section 32 AML/CTF Rules, Chapter 4	During the 2011 calendar year, Crown recorded the following breaches by its employees in respect of Crown's customer identification procedures: • 9 instances of a failure to record a residential address; • 10 instances of recording an expired ID; • 6 instances of an appropriate ID not being sighted; • 1 instance of an appropriate ID not being listed on Crown's internal records system; • 1 instance of no date of birth or expiry date being listed on the recorded ID;	While a number of the specific instances have been remediated, due to the passage of time Crown is not able to determine whether every instance was remediated.	January 2011 – December 2011	Please refer to row 2 of this table.

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 neither a name or residential address being recorded; • 4 instances of no residential address and no country of issuance on the recorded ID; • 1 instance of residential address of a customer only being recorded after the relevant transaction with a customer; and • 1 instance of a transaction that should not have been completed.			
4	AML/CTF Act, section 32 AML/CTF Rules, Chapter 4	During the 2012 calendar year, Crown recorded the following breaches by its employees in respect of Crown's customer identification procedures: • 8 instances of a failure to record a residential address; • 1 instance of recording an expired ID; • 7 instances of an appropriate ID not being sighted; • 1 instance on an appropriate ID not being entered on Crown's internal records system;	While a number of the specific instances have been remediated, due to the passage of time Crown is not able to determine whether every instance was remediated.	January 2012 – December 2012	Please refer to row 2 of this table.

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
		• 2 instances of a residential address only being recorded after a transaction had been completed.			
5	AML/CTF Act, section 32 AML/CTF Rules, Chapter 4	During the 2013 calendar year, Crown recorded the following breaches by its employees in respect of Crown's customer identification procedures: • 10 instances of a failure to record a residential address; • 5 instances of recording an expired ID; • 2 instances of an appropriate ID not being sighted; • 1 instance of a failure to record a date of birth; • 1 instance of a no ID being supplied by a customer; • 1 instance of failure to record a passport number; and • 1 instance of the identify of a third party conducting the transaction not being entered in Crown's system.	While a number of the specific instances have been remediated, due to the passage of time Crown is not able to determine whether every instance was remediated.	February 2013 – December 2013	Please refer to row 2 of this table.

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
6	AML/CTF Act, section 32 AML/CTF Rules, Chapter 4	During the 2014 calendar year, Crown recorded the following breaches by its employees in respect of Crown's customer identification procedures: • 3 instances of a failure to record a residential address; • 1 instance of recording an expired ID (although a current ID was sighted by a staff member); • 2 instances of an appropriate ID not being sighted; • 3 instances of a failure to record a date of birth; and • 1 instance of recording an ID that had no expiry date.	While a number of the specific instances have been remediated, due to the passage of time Crown is not able to determine whether every instance was remediated.	January 2014 – November 2014	Please refer to row 2 of this table.
7	AML/CTF Act, section 32 AML/CTF Rules, Chapter 4	During the 2015 calendar year, Crown recorded the following breaches by its employees in respect of Crown's customer identification procedures: • 14 instances of a failure to record a residential address; • 2 instances of a failure to record a date of birth; • 9 instances of recording an expired ID; and	While a number of the specific instances have been remediated, due to the passage of time Crown is not able to determine whether every instance was remediated.	January 2015 – December 2015	Please refer to row 2 of this table.

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 when a Government senior card was accepted as an appropriate ID from a customer.			
8	AML/CTF Act, sections 32 and 43 AML/CTF Rules, Chapters 4 and 19	During the 2016 calendar year, Crown recorded the following breaches by its employees in respect of Crown's customer identification procedures (and one threshold transaction reporting breach): • 5 instances of a failure to record a residential address; • 4 instances of a failure to record a date of birth; • 1 instance of a failure to record a customer name; • 4 instances of recording an expired ID; • 3 instances of when an appropriate ID was not sighted; and • 1 instance where a $10,000 transaction was not recorded and where the customer was unknown (as they were uncarded).	While a number of the specific instances have been remediated, due to the passage of time Crown is not able to determine whether every instance was remediated.	January 2016 – December 2016	Please refer to row 2 of this table.

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
2. Ongoing customer due diligence and record keeping					
9	AML/CTF Act, section 112	The Cage failed to input all information into SYCO on occasions and there were data entry errors. For example, PokerPro database information was not always placed into SYCO.	Corrective action taken in relation to data entry errors, with all issues being reported and reinforced with relevant management.	November 2010 – August 2011	The Crown Financial Crime Team had discussions with the Cage to ensure the issue did not reoccur. Relevant employees were also counselled. In addition, the auditing of PokerPro database information continued to be conducted to assess compliance.
10	AML/CTF Act, section 36	The Compliance Manager identified an issue which was not appropriately escalated by Security Services regarding theft (with the money stolen allegedly being subsequently gambled at Crown). The customer admitted to having gambled stolen money at Crown between 10 July 2011 and 6 August 2011. The delay meant that Crown may have continued dealing with the customer for longer than it should have under its AML/CTF Program.	Crown placed 'stop codes' on the customer's account and submitted an SMR. Security Services also subsequently requested an AML/CTF presentation to ensure they were across all the relevant obligations, which was provided.	August 2011	
11	AML/CTF Act, section 36 and 112	Crown identified that there was insufficient record keeping of due diligence checks conducted on junket operators and that formal documentation was not kept of the relevant processes.	In September 2014, Crown directed its staff that new junket applications must contain full details of the junket, including customer name, number, copy of passport, country and this was to be provided to Credit Control prior to executive approval and stored on a specific drive in VIP International.	December 2014	See 'Steps taken to remedy the breach or potential breach' column.

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
			This was formalised in a 'Junket Process' (internal processes and procedures) document. In November 2014 Crown also commenced ordering Wealth X reports in existing junkets of over $5 million.		
3. AML/CTF Program and compliance					
12	AML/CTF Act, sections 32, 36, 43, 45 and 81 AML/CTF Rules, chapters 4, 8, 15.9, chapter 17 and 19	In a Compliance Assessment AUSTRAC raised the following areas of non-compliance: • Crown Melbourne's AML/CTF Program did not refer to Crown's processes for reporting of IFTIs, TTRs and SMRs, its obligations regarding compliance reports or the systems or controls supporting that. • Crown's AML/CTF risk awareness training did not contain any material to enable its employees to understand the consequences of non-compliance with the AML/CTF Act and Rules. • The AML/CTF Program stated that ECDD is undertaken when an SMR is submitted. However, the AML/CTF Rules required that ECDD be applied when a	The Crown Melbourne Compliance Committee discussed the outcome of the compliance assessment and noted that AUSTRAC had stated that 'Crown demonstrated a strong compliance culture and concluded that no substantive or systemic issues of concern were evident.'	August 2011 and May 2012	Crown made a range of improvements to its AML/CTF Program on 11 October 2012 following the receipt of the compliance assessment, updated its online training program, refresher IFTI training, and communicated this update to AUSTRAC on 4 October 2012.

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
		suspicion has arisen for the purposes of s41 and not after an SMR has been filed. Furthermore, between 6 January 2012 and 1 May 2012, nine SMRs were reported in respect of a particular customer . Crown should have considered applying ECDD to determine whether a relationship should continue with the customer. • The residential addresses of some customers were not collected despite being part of the minimum required KYC information. • AUSTRAC identified a number of deficiencies in IFTI reporting, including (a) the name on an IFTI did not match the name on identification documentation; (b) some IFTIs failed to include residential address, date of birth, or identification information; and (c) some reports contained customer identification documents which did not meet the criteria of being 'reliable and independent' documentation.			

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
		• AUSTRAC identified a number of deficiencies in TTR reporting, predominantly data entry errors (e.g. inputting a name in the wrong field, or inputting the wrong name).			
13	AML/CTF Act, section 41 and 81 AML/CTF Rules, Chapter 18	As part of AUSTRAC's compliance assessment of Crown Melbourne, AUSTRAC noted that there were: • deficiencies in its risk assessment and AML/CTF Program regarding transfers from foreign jurisdictions (AUSTRAC noting this was outside the original scope of assessment); and • there were errors in SMRs involving the mapping of information to incorrect fields.	Crown informed AUSTRAC that it would take the following steps in response: • conduct further periodic risk assessments and consider whether additional measures (further ECDD, additional SMR reports where appropriate, etc.) need to be taken in connection with patrons and/or funds originating from certain jurisdictions (if that information is known to Crown Melbourne). • a periodic jurisdiction review will be formalised into the AML/CTF Program and it will take additional measures as appropriate and in accordance with countries identified in the period jurisdiction review. • when completing SMRs, it will ensure it includes all relevant information in the SMR and will include additional specificity relating	September 2013 to March 2014	See 'Steps taken to remedy the breach or potential breach' column

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
			to grounds of suspicion by selecting multiple codes in its SMRs where this is appropriate. • it has referred errors found in its SMR program and is in the process of investigating solutions to improve data capture and mapping functions. Additionally Crown added: • a SYCO alert and High Jurisdictional Risk to the profile of customers from Prescribed Foreign Countries and ensured that it considered a Customers jurisdictional risk when conducting his transaction monitoring' and • multiple 'reason for suspicion codes' in SMR reports where appropriate.		
14	AML/CTF Act, section 82 AML/CTF Rules, rule 8.2	An internal audit into Crown's compliance with its AML/CTF Program dated 25 January 2016 stated that nine employees failed to complete training on time. Of those nine, completion of the required training by seven overseas employees was outstanding due to restricted access to the online training platform.	Outstanding staff were enrolled in training commencing September 2016, with a requested completion date of November 2016.	25 January 2016	Crown proactively monitors compliance with training requirements and escalates to the AML/CTF Officer and/or CEO as required.
4. Reporting obligations					

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
15	AML/CTF Act, section 45	Four of 30 IFTI's sampled were not reported to AUSTRAC within the required 10 business day timeframe One IFTI was reported with the incorrect currency (reported in HKD not AUD).	The IFTI in the incorrect currency was recalled and resubmitted to AUSTRAC.	December 2009 -February 2010	The CTRM performed a follow up audit on a further sample of 40 IFTIs. No issues were identified.
16	AML/CTF Act, section 45	Crown identified the following issues in relation to IFTIs: • six instances (out of 48 transactions sampled) where IFTIs were not reported within 10 business days. • One instance where the beneficiary date of birth in an IFTI was reported incorrectly to AUSTRAC.	Crown took the following actions: • An IFTI audit was performed in January 2015 with no IFTIs exceeding the 10 business day reporting deadline. Management continued to monitor IFTI reporting in line with AML/CTF requirements. • The IFTI with the incorrect date of birth was resubmitted to AUSTRAC.	2014	See response for row 15 of this table.

Annexure 1 – SLE

Annexure 1

SURVEILLANCE LOG ENTRY REPORT

LOG DESCRIPTION (Intelligence Only)

Information received from a Surveillance source:

During LDP Learning Block 2 on 16/03/2021 one of the attendees, Premium Service Host [redacted], was heard to make a large amount of remarks relating to money laundering and Crown staff being aware and assisting in money laundering activities with patrons.

Before beginning in earnest [redacted] remarked "we're all Crown here, so I can talk about this".

[redacted] then went on to make the following claims (paraphrased).

-Crown staff, presumably talking about the hosting team, were aware that international patrons were engaged in money laundering activities. "We knew there was money laundering happening"

-Hosting staff were given instruction from "higher ups" to identify, implement or create new methods of circumventing "government laws" (spoken about in the context of money laundering)

-one method of money laundering involved international patrons getting in touch with patrons based out of Australia. The first patron would transfer money (example $5M) from their account in a Chinese bank to an account at a Chinese bank belonging to the second patron (based out of Australia). The second patron would then independently transfer the same amount from his account at an Australian Bank to an unspecified location in Australia (either an Australian bank account belonging to the first patron or straight to Crown as a 3rd party TT). This would prevent large amount of cash from crossing international lines, potentially allowing it to dodge additional government scrutiny.

- a second method involved having a high action international patron staying at a hotel (ie. Crown Towers). They (the hosting or hotel staff) would charge an "incidental charge" [redacted] failed to specify an amount) to the hotel invoice of the patron. The patron would then settle their hotel bill, including the incidental charge, using "tap and go". This would transfer money from an international account to Crown to settle the amount on the hotel room. The money for the incidental charge would then be made available to the patron, potentially at the cage, for the purposes of gaming.

[redacted] stated that the rules regarding the above were a lot looser prior to "China happening", relating to the detainment of a number of Crown, stating on more than one occasion "China changed everything".

There were fourteen staff members in attendance (including myself), plus the facilitator [redacted], whom the majority of the conversation was directed toward.
Also in attendance:

[redacted]

(others too, but did not have chance to grab names)

EVENT DESCRIPTION

SURVEILLANCE LOG ENTRY REPORT

DETAILS

Log ID	1984416	**Department**	Surveillance
Date	17/03/2021 09:04	**Event**	Intelligence
Parent Log ID		**SubEvent**	Rumour
		Game Type	

Area		**Amount Involved**	
Location		**Status**	Not Applicable
Reference		**Monitoring Type**	Administration

PATRONS INVOLVED

Name	Syco ID	Person ID
[redacted]		[redacted]

STAFF INVOLVED

Name	Employee ID	Job Title
[redacted]	[redacted]	Premium Service Host