Royal Commission into the Casino Operator and Licence

STATEMENT OF NICK STOKES

Name: **Nicholas St Aubyn Stokes**

Address: Crown Towers, Level 3, 8 Whiteman Street, SOUTHBANK VIC 3006

Occupation: Group General Manager Anti-Money Laundering and AML/CTF Compliance Officer

Date: 25 April 2021

1. I make this statement in response to the Royal Commission's Request for Statement - 007.

2. I hold a Master of Laws in International Relations from the Hitotsubashi University in Tokyo (2003) and a Juris Doctor from the University of Technology Sydney (2010). I also hold a Bachelor of Asian Studies (Japanese) from the Australian National University in Canberra.

3. I joined Crown on 19 November 2019 as the Group General Manager, Anti-Money Laundering. On 2 November 2020, I was appointed the AML/CTF Compliance Officer for the reporting entities within the designated business group.

4. Prior to commencing my employment with Crown, I held several roles in the banking sector:

    - between September 2016 and June 2019, I worked as the Head of Financial Crime Compliance for the Asia Pacific Region (excluding Singapore and Hong Kong) for Credit Suisse Services AG, Singapore Branch. In November 2018, I also took on the role of Head of Anti-Bribery and Corruption Compliance for the Region;

    - between March 2015 and September 2016, I worked as the Head of Anti-Bribery & Corruption for Standard Chartered Bank (ASEAN & South Asia) in Singapore;

    - between November 2013 and March 2015, I worked as the Regions Head of Financial Crime Compliance Assurance (Asia, Africa & Middle East); and

    - between October July 2008 and October 2013, I held roles with the Bank of Tokyo-Mitsubishi UFJ Limited). Between July 2008 and October 2010, I worked as the Head of Compliance (Australian and New Zealand), before transitioning to the Regional Head of Financial Crime Risk until October 2013.

5. I have also held roles with Australian regulatory bodies, most recently, at the Australian

Transaction Reports and Analysis Centre (**AUSTRAC**), where I worked as a Technical Advisor between September 2007 and July 2008. In 2005 and 2006 I also held roles with AUSTRAC as a Manager, Regulated Entities and as a Regulatory Supervisor, Reporting and Compliance.

6. In addition to my roles at AUSTRAC, I have held roles as a Senior Analyst both in Enforcement and in Policy Research & Statistics at the Australian Prudential Regulation Authority.

A. Manual transaction monitoring rule

55. Describe the operation of the newly adopted manual transaction monitoring rule.

7. In accordance with the *AML/CTF Manual Rule - Bank Statement Monitoring Policy* (CRL.742.001.0009), the existing manual monitoring refers to what the Financial Crime Team (**FCT**) are performing currently in terms of reviewing customer transactions (i.e. deposits and transfers) into Crown's ANZ bank accounts for the purposes of detecting three types of activity:

- possible cash deposits, including structuring or smurfing behaviour, by customers or third parties into Crown's bank account;
- electronic funds transfers (**EFTs**) by customers that contain transaction descriptions that are unrelated to gaming; and
- EFTs by third parties, including money remitters

where these are evident from the bank statement.

8. The FCT manually reviews the bank account statements line-by-line on a weekly basis to identify the above transactions. For a description of how this process works in practice and to understand the operational steps the FCT follow, reference is made to the *Crown AML Manual Bank Statement Review Guidelines* (CRW.510.039.3515).

9. The Financial Crime Team will continue the manual review of the bank statements until the automated exception flags are developed. Following implementation of the automated exception flags referred to below at #57, the VIP Banking team, as the operational first line of defence, will review the flags and follow the *Return of Funds Policy* (CRW.512.025.1110) requirements in the event that the activity mentioned above is detected. This may include submitting an Unusual Activity Report (**UAR**) to the FCT. Following implementation of the automated bank account flags the FCT will perform periodic sample testing as part of its second line assurance responsibilities.

56. Why is this rule being introduced?

10. The rule has been introduced as a detective control measure to mitigate and manage the potential money laundering risk that Crown may face with respect to:

- accepting cash deposits by unknown third parties or customers where the source of funds is unknown or potential proceeds of crime;
- EFTs that are referenced as being unrelated to gaming in an attempt to conceal the true intent behind the transfer; or
- facilitating third party payments (including money remitters) where the source of funds may not be known, including the profile of the person sending or receiving the payment.

57. Why is the transaction monitoring rule manual and not automatic?

11. Until quite recently Crown has not had the ANZ bank data file feeds to enable automated monitoring of bank statements.

12. I am informed by my colleagues in the Enterprise Reporting team (a financial reporting function) that the VIP Banking team in consultation with the Enterprise Reporting team are currently working on developing automated flags in the TM1 system. TM1 (formerly known as IBM Planning Analytics) is a technology solution for financial reporting and spreadsheet analytics. In the context of bank statement monitoring, it acts as a user interface for matching bank deposits in the Crown ANZ account with transfer acknowledgement information recorded in the casino management system, SYCO. The TM1 system will also be used to keep track of funds being returned to customers under the Return of Funds Policy.

13. Crown has been working with ANZ on obtaining the relevant bank files since 21 December 2020. Since 12 March 2021, Crown is able to receive bank data file feeds from ANZ. Currently, the status of the development of the automated exception flags is about two-thirds complete. I have also been informed that user acceptance testing will commence in May 2021 and a parallel run of the old (manual) and new (automation) is due to start in June 2021.

58. Who will perform the manual transaction monitoring, and how frequently?

14. As outlined in #55 above, the FCT will perform the manual monitoring weekly until the exception flags have been automated which will include user acceptance testing.

59. What reports if any will result from the manual transaction monitoring?

15. As outlined in #55 above, the FCT will undertake a line-by-line analysis of each statement to identify potential unusual activity. If the FCT Team identifies such a transaction and the transaction has not already been subject to an UAR from the Cage the team will internally generate a UAR which will then be triaged or investigated in line with the UAR/SMR framework outlined in the Joint AML/CTF Program (CRW.514.002.0110).

B. Third Party Transfers and Money Remitters Policy

60. Describe the operation of the Third-Party Transfer and Money Remitters Policy.

16. The *Third Party Transfer and Money Remitters Policy* (CRL.742.001.0101) governs the operation of third party payments and transfers (including to and from money remitters).

17. In accordance with this policy, 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

unless prior written approval for the relevant transfer has been obtained from the property Chief Operating Officer (now Chief Executive Officer) and Group AML/CTF Compliance Officer.

18. Although not attached to the abovementioned Policy, an Executive Office Memorandum (**EOM**) was issued as a form of guidance by the Perth and Melbourne Chief Operating Officers on 21 October 2020 (CRW.520.003.9552). In terms of what constitutes a third party transfer, the EOM contained a number of responses to frequently asked questions (FAQs), one of which relates to whether Crown can send or receive funds to or from other casinos. This was answered in the affirmative and is permitted on the condition that the ultimate transferor and the ultimate transferee are the same person. In practice, to date, only funds to or from Australian based casinos have been accepted.

61. Why is this policy being introduced?

19. The *Third-Party Transfer and Money Remitters Policy* was introduced to give formal effect to the EOM titled *Prohibition on Third-Party Payments* (CRW.512.027.1026) issued by the then Australian Resorts CEO Mr Barry Felstead on 8 April 2020.

20. That EOM was issued to document the directive by the Australian Resorts CEO to prohibit third party payments arising out of a number of meetings held in March 2020 between the CEO and other senior Crown executives and Business Operations Team members on the risk of third party payments to Crown particularly in respect of the money laundering risk.

62. When was it introduced?

21. The *Third-Party Transfer and Money Remitters Policy* was introduced on 16 November 2020.

63. What is the role of property CEO?

22. The role of the property CEO in the context of the *Third-Party Transfer and Money Remitters Policy* is the ultimate approver of a third party transfer exception. The reference to 'property' CEO is to distinguish between the three CEOs, each for Melbourne, Perth and Sydney.

64. What criteria must the property CEO apply to give written approval for Third Party Transfer into Crown's bank accounts.

23. There is no formal criteria, rather the property CEO will consider the written recommendation prepared by the respective business unit (e.g. Table Games, Gaming Machines and VIP International) and reviewed by the AML/CTF Compliance Officer to determine whether the third-party transfer should proceed. Reference should also be made to paragraph 25 below in #66.

65. Who is the Crown AML/CTF Compliance Officer?

24. I currently hold the position of AML/CTF Compliance Officer.

66. What criteria or considerations may the AML/CTF Compliance Officer apply to give written approval for Third Party Transfers into Crown's bank accounts.

25. In accordance with the *Third-Party Transfer and Money Remitters Policy*, any departure from the default position (i.e. prohibition) will need to satisfy the defined criteria outlined in the policy.

26. The relevant business unit (e.g. Table Games, Gaming Machines and VIP International) must collate certain information required by the policy and provide to FCT who will then provide a third party transfer recommendation for the AML/CTF Compliance Officer to approve or not approve.

27. The AML/CTF Compliance Officer will take into consideration the following criteria:

- details of the customer and the third party involved in the transfer;
- information in relation to the third party's connection to, and relationship with, the customer and purpose of the proposed transfer;
- a summary of recent gaming activity (including any transfers to or from their patron account);
- the history of the customer's risk ratings within Crown, including (if applicable) the dates and reasons for the escalation of the customer's risk rating;
- a summary of any historical adverse information held about the customer, including the results of Dow Jones screening (Crown's watch list and adverse media tool);

- a statement of the business rationale for departing from the default position;
- the AML/Financial Crime Team's views on the money laundering and terrorism financing (**ML/TF**) risks presented by the proposed transfer; and
- the AML/Financial Crime Team's recommendation as to whether the proposed transfer should proceed, having regard to the ML/TF risks presented by the proposed transfer.

28. Having considered the factors set out above, the AML/CTF Compliance Officer will then make a recommendation to the respective property CEO.

67. Have any prior written approvals for Third Party Transfers into Crown's bank accounts been made since the adoption of the new policy?

29. Yes.

68. If yes, please describe the circumstances of those approvals.

30. On 25 November 2020, the VIP International Team received a request from a Junket Representative for a Junket Operator to transfer winnings and front money from their last program (pre-COVID-19) to a Key Player.

31. The VIP International Team sought approval to complete a third party transfer for the net amount of $215,525 (comprising a front money component of $180,000, winnings of $262,000 less mid program cash-outs of the Key Player).

32. The VIP International Team were able to verify that the transfer was to be made to the Key Player's bank account as it had the Key Player's bank details from the original telegraphic transfer of the $180,000 front money.

33. The FCT confirmed the details VIP International's request (aside from the $15,000 cash out) and also noted:

- a history of large losses and a third-party transfers where the relationship was unknown;
- no hits on a Dow Jones/Factiva Negative news search;
- appeared to have been fined CNY100k (approximately $20,000) in 2016 for breaching trading regulations, as noted in a WorldCheck match;
- Crown had previously obtained a Wealth X third party due diligence report that estimated the customer's net worth at approximately $30m; and
- Crown had no record of law enforcement agency enquiries noted on file.

34. The FCT consulted with the Crown Melbourne Table Games Gaming Integrity Manager, who advised that there was no other adverse information on the customer.

35. In my capacity as the AML/CTF Compliance Officer and under the EOM, I approved the third-party payment.

36. I am informed by my colleague Mr Stephen Hancock, General Manager, Cage and Count Melbourne, that on 6 April 2021, a third party transfer was inadvertently processed by Cage staff in breach of the Third-Party Transfer and Money Remitters Policy. The transfer involved a payment from a Crown customer to his wife (also a Crown customer) representing the proceeds of the husband's domestic program settlement.

37. When the Cage staff processed the transfer they input the information in the casino management system, SYCO, from a previous telegraphic transfer processed in February 2020 which automatically populated the customer's wife's details. Cage staff incorrectly assumed their account was a joint account without confirming as such with the customers first, both of whom were present at the Cage at the time of the transfer.

38. I am further informed that the breach was initially detected by the Cage and Count Melbourne team's Finance Integrity Manager after processing of the transfer. The breach was also detected by the FCT's automated second line assurance monitoring. The Cage staff involved attended a disciplinary meeting on 19 April 2021 and received a written warning. The Policy requirement was also reinforced at that meeting and acknowledged by the staff involved. As a result of this incident, the Cage has introduced a further control on 22 April 2021 to the effect that no outgoing transfer is to be processed by VIP Banking until the Cage and Count Finance Integrity Manager has reviewed the transfer.

C. Development of automated transaction monitoring rules

73. Describe the operation of any new automated transaction monitoring rules.

39.

40.

41.

42. [redacted]

43. [redacted]

44. [redacted]

45. [redacted]

46. [redacted]

47. [redacted]

48. [redacted]

49. [redacted]

50.

B. Financial Crime Resourcing and Team Structure

87. In respect of each of the new financial crime roles referred to, have the persons involved been employed on permanent or fixed term contracts?

51. Permanent contracts, with only one role occurring on a fixed term basis.

88. If fixed term, please state the term of the contracts?

52. The Financial Crime - Project Manager is currently a contract role until at least 30 June 2021.

89. Describe the number of FTE roles in the Financial Crimes team pre and post the creation of these new roles.

53. Before the creation of the new roles the number of FTE in the Melbourne and Perth teams totalled 6. As of 21 April 2021, the Financial Crime Team is made up of 20 approved FTE roles and one fixed term role.

E. AML reporting structures and governance

97. How were matters now dealt with by the newly established AML/CTF Committee dealt with prior to the establishment of that committee?

54. The current iteration of group-wide AML/CTF Committee was an initiative implemented by me shorty after my appointment to the role. My predecessor had set up a group-wide committee

during 2019, however a formal charter was not adopted.

55. I am informed by my colleague Mr Adam Sutherland, Group Senior Manager Financial Crime that prior to the formation of the group-wide committee in 2019, Crown Melbourne held a standalone or property-specific AML/CTF committee while for Crown Perth, the former AML/CTF Compliance Officer held regular recurring meetings with the Perth AML Team. According to the 26 September 2019 Committee Preliminary Meeting minutes the attendees were invited to explore an appropriate composition and terms of reference and noted the operational and risk focus of the Committee going forward. Further, it was outlined that the Committee would comprise Crown senior management from the business units so that important AML/CTF matters could be communicated.

D. Enhanced Patron Account Controls

106. What were the results of Crown's 'lookback' of the transactions identified in the reviews of the Riverbank and Southbank accounts?

56. An internal investigation was launched on or around August 2020. Mr Claude Marais, General Manager - Legal and Compliance (Crown Perth) prepared a memorandum providing an update on the internal investigation to Mr Ken Barton, Chief Executive Officer (Crown Resorts Limited) dated 29 September 2020 (CRL.729.021.2371), a relevant extract from item 5 of the memorandum shows a summary of the results:

	Riverbank	**Southbank**	**Total**
Number of instances	84	18	102
Number of cash deposits	429	180	609
Number of patron accounts to which the deposits were credited	51	10	61

57. Following the internal investigation, Crown engaged Grant Thornton on 14 October 2020 to:

(a) validate the investigation set out in Mr Marais' memorandum referred to above; and

(b) perform an analysis of bank statement data to identify potential "structuring" transactions involving the Riverbank and Southbank accounts (Phase 1).

58. The results of the 'lookback' exercise titled Forensic Data Analysis for Crown Resorts

Riverbank Investment Pty Ltd and Southbank Investment Pty Ltd – Final Reports have been provided to the Commissioner (CRW.510.001.0001 and CRW.510.001.0031).

59. Crown further engaged Initialism with support from Grant Thornton to perform an analysis of bank statement data for other AML/CTF typologies which may be indicative of money laundering / terrorism financing risks (Phase 2). The report can be found at (CRW.510.001.0049).

60. The Financial Crime team is currently reviewing these typologies and transactions to determine what has already been reported to AUSTRAC and what further reporting to AUSTRAC is required.

107. What, if any, further reporting to AUSTRAC occurred as a result of the lookback?

61. Crown, as part of Phase 1 referred to above in #106, submitted 51 SMRs to AUSTRAC in respect to Riverbank Investment Pty Ltd and submitted eight (8) SMRs in respect of Southbank Investment Pty Ltd.

62. Crown, in relation to Phase 2, has submitted five (5) SMRs to AUSTRAC at the time of making this statement in line with the Initialism and Grant Thornton reports. Crown continues to perform the lookback, prioritising structured cash deposits, quick cash deposits and third party transfers consistent with the cuckoo smurfing typology. If further suspicions are formed Crown will submit additional SMRs to AUSTRAC.

108. Describe the challenges in eliminating cash deposits by patrons at ANZ branches?

63. [redacted]

64. A secondary challenge is the ability to identify actual cash deposits into Crown's ANZ bank account from the bank statement. Based on previous discussions with ANZ, cash deposits will potentially show up on the statement as either BAI 366 code or AGT transaction type code. Bank Administration Institute (BAI) codes are unique identifiers used by financial institutions that differentiate the types of transactions that are posted to an account. For example, BAI 366 code refers to currency and coin deposited. However, based on Crown's experience to date with reviewing bank statement data files with the above codes it is not conclusive that these codes are, in all instances, a reference to cash deposits. This understanding has been confirmed by ANZ that advised that there is no definitive flag available to Crown for use as a marker for cash deposits.

109. What are the options to address this issue?

65. In response to the abovementioned challenge Crown has undertaken the following four initiatives:

#1 – Email communication to Crown customers

66. I am informed by Mr Phillip Batsakis, Group Commercial Manager, VIP International, that letters were sent to VIP International premium player customers and junket operators who resided in Hong Kong and Macau in late September 2020 advising that cash deposits into Crown bank accounts are no longer permitted by Crown.

67. I have seen a broadcast email dated 24 December 2020 (CRW.512.040.0001) jointly authored by Mr Tim Barnett, Executive General Manager, Table Games, and Mr Mark MacKay, Executive General Manager, Gaming Machines. The authors wrote to its premium members advising, amongst other things, that Crown will no longer release cash deposits that are made into Crown bank accounts.

#2 – Development of automated exception flags to identify potential cash deposits

68. I am informed by the Enterprise Reporting team that they, in consultation with the VIP Banking team, are developing additional automated exceptions flags to identify the types of transactions on Crown customer accounts that fall within the ambit of the Return of Funds Policy, including cash deposits. These automated flags, based on matching criteria from the ANZ daily bank data feeds, will trigger a review of the particular transaction and allow the VIP Banking team to action any non-compliance with the Return of Funds Policy. In addition, any identified unusual or potentially suspicious activity will be escalated to the Financial Crime Team via a UAR. Until this capability is implemented, the Financial Crime Team will continue to conduct weekly manual bank statement reviews in accordance with the Manual Bank Statement Review Guidelines.

#3 – Introduced certain consequences for customers who make a cash deposit based on the Return of Funds policy

69. [redacted]

#4 – Ongoing collaboration with ANZ

70. The FCT continues to meet with the ANZ Financial Crime team periodically to discuss and address issues or concerns relating to any identified anomalies detected in the bank account

monitoring performed by Crown and continue to explore further opportunities for collaboration around managing and mitigating ML/TF risk for both Crown and ANZ.

E. Transaction monitoring program / Sentinel

110. What are the limitations of the Sentinel program?

71. [redacted]

72. [redacted]

73. [redacted]

111. How does Crown propose to address those limitations?

74. 

75. The Financial Crime Team also has access to the following full-time dedicated resources from the IT Sentinel team:

- four (4) developers building new rules and making enhancements;
- two (2) quality assurance analysts conducting due diligence, including data integrity checks;
- one (1) technical lead providing oversight; and
- one (1) project manager or business analyst.

112. What is the status of the roll-out of Sentinel? Is it complete? How long has it taken to roll out Sentinel?

76. Sentinel was rolled out on 2 February 2021. Although further rules and adjustments to existing rules are being considered currently there are 24 rules now in operation. In accordance with the Joint Program, Crown will review, test and refine its TMS periodically. This will include focusing on alert effectiveness, including understanding the productivity of alerts generated during the review period. Crown has also deployed the first iteration of the RBA model as described above in #73.

77. I am informed by my colleague, Mr Puneet Talwar, General Manager, Centralised Platforms that the AML Sentinel Program was originally put forward at an Executive Briefing (CRW.510.013.1280) in August 2018. According to the briefing document, at that time Sentinel

was conceived as a piece of technology using Splunk to address the manual nature of the monitoring and assurance work that was being performed. The AML Sentinel Program was pitched as being an operations integrity solution for regulatory reporting, investigation support (via customer and transaction monitoring) and business risk insights. I am further informed that in February 2019, work started on building the foundations of the overarching Sentinel framework which included the creation of transaction and other data logs that could be fed from source systems to the Sentinel rules engine in Splunk. Work on the Sentinel platform continued to evolve from that date until the present.

113. How long will it take for the dispositioning and triage process to become digitised?

78. The digitised dispositioning and triage process of UARs in the AML Portal went live to the business on 12 April 2021. The development of digitised dispositioning and triage of Sentinel risk-based alerts through the AML Portal will commence following the first release of the of the AML Portal.

79. I am informed by my colleague, Mr Puneet Talwar, General Manager, Centralised Platforms that it is anticipated that it will take 3 months for the auto-creation of digitised Sentinel Alert (UAR) each time an RBA alert triggers. The UARs will be dispositioned in Crown's (digital) AML Portal.

114. What conclusions and/or recommendations did Initialism make pursuant to its transaction monitoring source information review?

80. Crown received a draft *Transaction Monitoring Program Review* from Initialism due to Initialism on 20 April 2021 (CRW.512.039.0062).

F. Regulatory reporting

115. Why was a UAR process introduced?

81. Historically Crown's SMR process has been largely paper based and involved:

- frontline staff raising an Internal SMR form to the AML Team which was supplemented, where possible, with relevant additional information prior to being reported to AUSTRAC; and
- the AML Team submitting an SMR following review of daily / weekly / monthly manual transaction reports based on known or published casino ML/TF red flags or typologies.

82. Shortly after joining Crown in mid-November 2019, I performed a limited and informal sample review of Crown's Internal SMRs (as they were then called) including a review of the end-to-end process. I was also informed by AUSTRAC feedback as to the quality and content of a

sample of both Crown Melbourne and Perth property SMRs received in August 2017. I decided to overhaul the end-to-end process of Crown's Internal Suspicious Matter reporting and introduce an UAR framework. I modelled the UAR process based on my experience of how the process works in the global banks that I had previously worked at.

83. The new UAR framework is designed to be a three-level end-to-end investigative process: Level 1 (initial UAR review or triage); Level 2 (investigation); and Level 3 (the decision whether to submit an SMR to AUSTRAC).

116. Was it introduced at the recommendation of a person or entity, and if so, who?

84. As mentioned above, it was introduced as a result of my sample review of the existing process.

117. What conclusions or recommendations if any have arisen from the pilot of digitised UAR process?

85. I am informed by my colleague Jon Yeats, Group Senior Manager Financial Crime – Customer Investigations that the digitised system meets the key intended design requirements.

Key conclusions from the pilot are:

- Increased efficiency in administration of UAR reviews and investigations. The move to a more automated process removes the need to create, save and store template documents. It is anticipated that this will reduce timeframes within which UAR reviews and investigations are completed.

- Improvements in the tracking and auditing of timeframes for completion of UARs and cases. Previously, reporting could only show the creation and completion date of a UAR as it progressed through the various stages and decision points.

- Ability to extract and analyse collected data from the entire UAR process. The creation of thematic data points that are easier to extract and analyse. For example, data regarding emerging money laundering red flags or indicators could previously only be retrieved and analysed by manually extracting from Word template documents.

- The digitised process is not a complete overarching case management system as initially envisaged within which all relevant processes are undertaken. For example, it does not have a tasking capability and cannot track outgoing requests for additional information, this must still be done by email.

86. While the platform in its current state delivers a significant improvement from the previous manual process, there are already a number of further enhancements identified that Crown will explore as part of continuous improvement, including:

- To develop a tasking capability within the digitised platform or one that integrates with a case management system;

- An ability to construct a single view of customer's risk information – for example, build interconnectivity within existing Crown systems and using entity resolution and link identification to view potentially unknown or hidden associations between customers and events; and
- To design and develop a digitised form for the preparation and submission of an SMR to AUSTRAC.

118. Which external bodies or entities are conducting the external reviews of:

(a) IFTI reporting?

87. Initialism and Allens Linklaters.

(b) SMR reporting?

88. Allens Linklaters.

(c) TTR reporting?

89. Allens Linklaters.

119. When will those reviews be complete?

90. Crown received two draft reports from Initialism (who had conducted a limited desk-based review of Crown's compliance with IFTI reporting requirements (CRW.512.027.0332 and CRW.512.027.0626). Due to the limited size of the sample period (i.e. only March 2020 IFTIs), Crown has engaged Allens Linklaters to perform a further review of IFTI reporting as well as complete the other two reviews. We anticipate receiving the results by the end of Q3, 2021.

G. ECDD/KYC

120. What is being done differently at Crown in light of the introduction on 12 November 2020 of the Escalation of Critical Risk Customer Policy?

91. Until the adoption of the Escalation of Critical Risk Customer Policy (CRL.742.001.0026), the issue of customer retention was handled in accordance with the Person of Interest (POI) Committee Charter. Standing members of the POI Committee had voting rights in terms of whether a Crown customer would receive a Withdrawal of Licence (**WOL**) due to presenting an unacceptable risk to Crown. Further, with the adoption of the new AML/CTF Program, in particular, a Crown customer can be assessed as 'Critical risk' and as a result the customer will be treated under the Escalation of Critical Risk Customer Policy. Under this Policy, the

default position for critical risk customers is that in the absence of an AML Recommendation containing an ML/TF risk mitigation plan approved by the AML/CTF Compliance Officer, the customer is to be exited - i.e. receive a WOL.

121. What if any decisions as to customer retention have been made pursuant to that new policy?

92. Two customers have been rated as critical risk since November 2020. These customers were referred to the POI committee and subsequently had their licence to enter the property withdrawn.

122. How do decision as to customer retention differ under the new policy?

93. As set out above in response to question 120.

H. AML/CTF training

123. Who revised the online awareness training module?

94. The FCT, Crown Learning and Development Team, and PTA Consulting were jointly involved in the revision of the online AML/CTF Risk Awareness training module. The targeted audience for the online module is all Crown employees, including contractors.

124. How long on average does it take to complete the training module?

95. I am informed by my colleague, Mr Shane Thomas, Group General Manager of Learning and Development, that the training module takes approximately 20 minutes to complete. Further, I am informed that this duration is in line with industry best practice for online training module design which states 30 minutes is about the maximum, and less than 15 is too short. In the case of Financial Crime, targeted training is also provided to select business units, including Table Games (including VIP International), Gaming Machines, Cage, Security and Surveillance, Hotels and Food & Beverage. Targeted training can take between 45 to 60 minutes to complete.

125. Is there any assessment at the conclusion of the training module?

96. I am informed by my colleague, Mr Shane Thomas, Group General Manager of Learning and Development, that all Crown Learn modules have some form of assessment that employees must complete to ensure that they can demonstrate a certain level of understanding of the target content. Each module is designed to include a number of ‘knowledge checks’ as employees proceed through it. Knowledge checks are quizzes that are designed to give an employee an idea of how well they know the material and are used as progressive feedback that can assist the employee in helping them understand what they need to know and where

potential gaps (if any) may be in their understanding. In the case of the AML Online module there are series of assessment questions that employees need to correctly answer to demonstrate they have an understanding of AML/CTF risk awareness.

126. How does Crown measure whether the training module has been successful?

97. I am informed by my colleague, Mr Shane Thomas, Group General Manager of Learning and Development, that the Crown Learn team measures the success of a particular module by reviewing the training completion rates across all business units and through the receipt of feedback provided by Crown employees who have completed the training.

98. FCT also plans to use the AML Portal data as an indicator of potential effectiveness following targeted training to see if there are any UAR spikes involving that targeted audience.

127. Who conducted the face-to-face AML/CTF training with the C-suite executives?

99. I presented a session on 9 December 2020, with my colleagues Mr Sutherland and Mr Yeats, to the Business Operation Team (**BOT**) in Melbourne, which includes C-Suite executives. I also delivered identical sessions for Perth and Sydney BOTs.

128. Who conducted the face-to-face AML/CTF training with the board?

100. Mr Blackburn presented the face-face training to the board on 8 March 2021 with further input provided by Mr Haig and Mr Kerrigan of Allens Linklaters.

I. Employee due diligence

129. What were the results of the Dow Jones screening of moderate and high risk employees?

101. An initial screen on over 6,100 employees (largely Casino Licensed employees) was undertaken on 20th October 2020 against the Special Interest Person category in the Dow Jones Risk and Compliance Database. Following screening 30 potential matches were recorded against the Special Interest category in the Dow Jones Risk and Compliance database. 28 of the potential matches were assessed as false positives. The remaining two positive matches were previously known to Crown.

[redacted]

Date: 25 April 2021