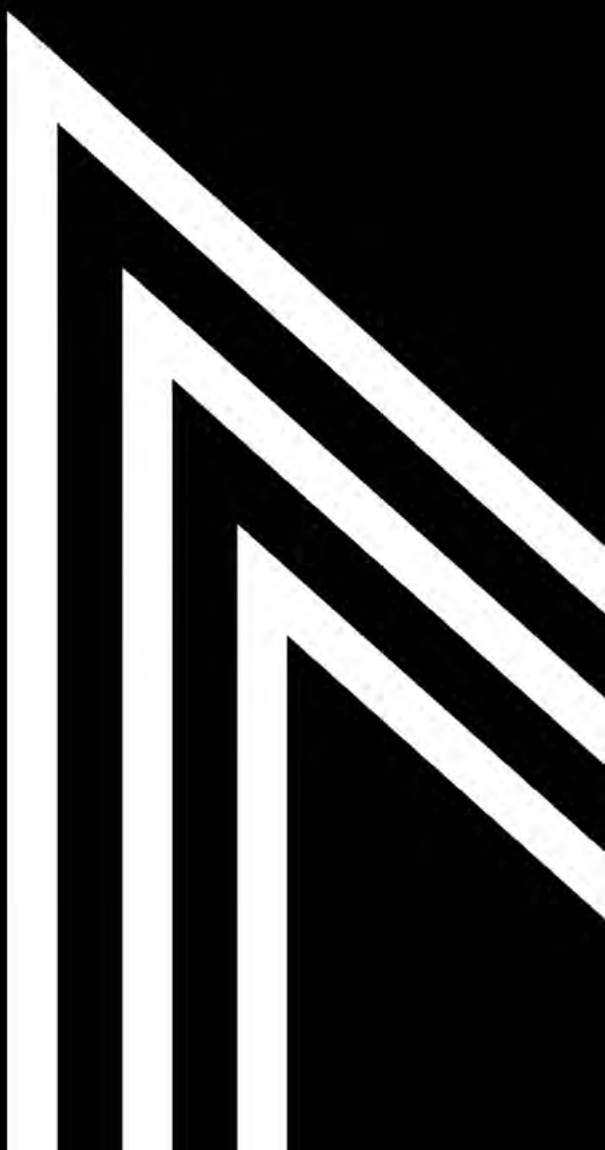
Royal Commission into Casino Operator and Licence

Forensic review – AML/CTF

5 July 2021



McGrathNicol

Contents

Appendices

Glossary of terms and abbreviations

Term	Meaning
ACM	Assistant Casino Manager
ACIP	Applicable Customer Identification Process
Allens	Allens Linklaters acting for Crown
ANZ	Australia and New Zealand Banking Group
AML	Anti-Money Laundering
AML/CTF Act, the Act	Anti-Money Laundering and Counter-Terrorism Financing Act 2006
AUD, A$	Australian dollar
AUSTRAC	Australian Transaction Reports and Analysis Centre
Bergin Inquiry	New South Wales Independent Liquor and Gaming Authority Inquiry into Crown Sydney to hold a restricted gaming license (Inquiry under section 143 of the Casino Control Act 1992)
Bergin Report	Report of the Bergin Inquiry dated 1 February 2021
Cage	The cash desks within the casino where customers may exchange chips and TITOs for cash, transact on their DAB accounts, exchange notes and currency
Casino Control Act	Casino Control Act (1991) (Victoria) as amended
CCFCO	Chief Compliance and Financial Crime Officer
CBA	Commonwealth Bank of Australia
CDD	Customer due diligence
chips	Physical tokens issued by each Crown casino
Commissioner	Raymond Finkelstein QC - Commissioner and Chairperson of the Royal Commission
Corrs	Corrs Chambers Westgarth
Counsel Assisting	Adrian Finanzio SC, Penny Neskovcin QC, Geoff Kozminsky and Meg O'Sullivan – each Counsel Assisting RCCOL
CML	Crown Melbourne Limited, the licensee of the Melbourne Casino
Croupier	Casino employee who runs a table game, also referred to as a dealer
Crown	Crown Resorts Limited and related and associated entities
Crown Resorts	Crown Resorts Ltd
Crown Sydney	Crown Sydney Gaming Pty Ltd
CSEL	Casino Special Employee Licence
CTF	Counter-Terrorism Financing
Customer	Used interchangeably with 'patron'
CVI	Casino Value Instrument
DAB Account	An account of funds advanced by a patron to Crown for the purposes of accessing for gaming
DAB balance data	DAB account data comprising the balance of all patron DAB Accounts with balances as at 15 June 2021, received by McGrathNicol from Crown on 18 June 2021
DAB transaction data	DAB account data comprising all transactions recorded for Patron Accounts in the period 1 January 2019 to 15 June 2021, received by McGrathNicol from Crown on 18 June 2021
DBG	Designated business group

Term	Meaning
DD	Due diligence
Dealer	Casino employee who runs a table game, also referred to as a croupier
the **Deloitte Report**	Phase 1 Report dated 26 March 2021 in which Deloitte provides an independent assessment of the design and operation effectiveness of controls in respect of patron accounts (DTT.005.0001.0038)
DOB	Date of birth
eTG	Electronic table game including semi–automated (where a live croupier deals the or spins the roulette wheel but players place bets on an electronic device) and fully automated where the deal, spin and bets are all electronic
ECDD	Enhanced customer due diligence
EGM	Electronic gaming machines, also knowns as pokies, poker machines, slots or slot machines
EOM	Executive Office Memorandum
EWRA	Enterprise-Wide Risk Assessment
FCCCP	Financial Crime and Compliance Change Program
FCP	Financial Crime Program
Gaming floor	Gaming floor includes all areas of the Crown casino complex which are licensed for the conduct of gaming activities
HKD	Hong Kong dollar
ILGA	Independent Liquor and Gaming Authority (New South Wales)
Initialism TM Report	Initialism's report dated April 2021 in relation to its review of Crown's Transaction Monitoring (INI.0004.0001.0172)
KYC	Know Your Customer actions and requirements under the AML/CTF
McGrathNicol	McGrathNicol Advisory
Melbourne Casino, the Casino	Casino located at 8 Whitman Street, Southbank and operated by Crown Melbourne Limited under a licence granted pursuant to the Casino Control Act 1991
Member	Member of Crown Rewards loyalty program
ML	Money laundering
OCDD	Ongoing customer due diligence
OTF	On the floor meaning in the Gaming floors in the casino
Patron	Used interchangeably with 'customer'
Patron Account	A Crown bank account into which patrons can deposit funds to credit to their DAB Account
PBA	Patron bank account
PBA data	The Patron Bank Account transaction data provided to Deloitte by Crown for all Patron Bank Accounts for the period 1 July 2019 to 22 February 2021 received by McGrathNicol on 23 June 2021
PEP	Politically exposed person
POI	Person of interest (generally in the context of a person whose behaviour is under scrutiny for the purposes of determining whether to issue a WOL).
Promontory	Consultancy firm, Promontory Australasia (Sydney) Pty Limited
the **Promontory Report**	Phase 1 report dated 24 May 2021 in which Promontory provides an independent assessment of Crown's AML vulnerability (CRW.512.086.003)

Term	Meaning
RBA	Rules based assessment
RCCOL	Royal Commission into the Casino Operator and Licence
Rewards, Crown Rewards	A loyalty program through which members can earn points to redeem for goods and services if they present their card whilst gaming or purchasing goods and services
Riverbank	Riverbank Investments Pty Ltd – subsidiary of Crown Resorts Ltd
Rules	Rules under AML/CTF Act
Sentinel Rules	Rules within the Sentinel program to match current and emerging ML/TF typologies and risks as they are described by the relevant peak bodies (such as AUSTRAC)
SPR	Significant Player Review
SK	Safe-keeping accounts
SMR	Suspicious Matter Report
SOF	Source of funds
Solicitors Assisting or SA	Solicitors to the RCCOL, Corrs Chambers Westgarth
SOP	Standard Operating Procedure
Southbank	Southbank Investments Pty Ltd – subsidiary of Crown Resorts Ltd
SOW	Source of wealth
SYCO	The casino management system
TA	Transfer Acknowledgement
Table games	Gaming undertaken at tables; includes baccarat, blackjack, roulette, poker
TF	Terrorism Financing
TITO	Ticket-in ticket-out
TRT	Ticket redemption terminal
TTR	Threshold Transaction Report
UAR	Unusual Activity Report
VCGLR	Victorian Commission for Gambling and Liquor Regulation
WOL	Withdrawal of Licence – an exclusion from the premises initiated by Crown
2LD	Second line of defence

1 Executive Summary

1.1 Scope of investigations, review and report

1.1.1 The scope of our work covers the key areas of interest shown in Table 1 as instructed by the solicitors assisting the Royal Commission into the Casino Operator and Licence (**RCCOL**).

Table 1

Area of interest	Matters addressed
Indications of money laundering on Patron Accounts	Addresses the finding of the independent inquiry conducted by Patricia Bergin pursuant to s143 of the Casino Control Act 1992 (NSW) that there had been indications of money laundering in certain bank accounts controlled by Crown.
Review new AML (Patron Account) controls	Addresses the effectiveness of new controls implemented to mitigate the risk of money laundering through Crown accepting deposits from patrons.
Analysis of patron transactions	An analysis of the transactions recorded in the Patron Bank Accounts and recorded in Patron DAB accounts for the period from 1 July 2019 to identify transactions which are potentially indicative of money laundering.
Transaction Monitoring Processes	Addresses the processes undertaken to monitor transactions to identify money laundering indicative transactions or behaviours, specifically the status and likely effectiveness of the recently introduced automatic monitoring tool, Sentinel.
Know Your Customer (**KYC**)	Addresses KYC processes and controls and assesses their adequacy and compliance with legislative requirements.
Financial Crime and Compliance Change Program (**FCCCP**).	Considers the current state assessment of Crown's Financial Crime and Compliance functions as assessed by Crown's recently appointed Group Chief Compliance and Financial Crime Officer, Steven Blackburn, and assesses the key elements of and risks to the pathway to uplift Crown's anti-money laundering functions as proposed in the Financial Crime and Compliance Change Program.
Money laundering "on the floor" (**OTF**)	Addresses the risks of money laundering occurring on the gaming floors of the casino and the controls in place to mitigate the risks and deter, detect and report incidences of money laundering indicative transactions or behaviours.

1.1.2 In accordance with our instructions our work has focussed on the current and proposed future state of Crown's operations and accordingly, we have not investigated past issues except:

(a) To the extent necessary to inform the extent of change recently implemented or proposed; and

(b) In respect of the look back at patron transactions in the bank accounts and DAB accounts.

1.2 Overview of work performed

1.2.1 The scope has been addressed by undertaking the following investigative procedures:

(a) Desktop review of relevant documents obtained from various parties under notices to produce issued by the RCCOL and provided to McGrathNicol by the Solicitors Assisting the RCCOL:

(b) Guided tours of the Melbourne Casino.

(c) Interviews with a number of senior employees.

(d) Issue of questionnaires which were completed by certain senior and management employees.

(e) Survey of significant number of floor staff.

(f) Survey of second line of defence staff.

(g) Focus group discussions with small groups of Crown Casino floor staff.

(h) Focus group discussion with a small group of Crown employees with roles involving AML control oversight.

1.2.2 In the course of our work we have experienced full co-operation and timely assistance from Crown personnel and Allens Linklaters (acting for Crown) as required to set up the interviews, surveys and focus groups.

1.3 Context and reliance on work of others

1.3.1 Our review has been undertaken in a dynamic environment which has influenced our approach.

1.3.2 During the course of our engagement, Crown has been undergoing significant internal review and changes have been made to personnel, reporting structures, policies and processes relevant to our work.

1.3.3 We have referenced several documents prepared by Crown in respect of these reviews and changes to inform our work, specifically:

(a) Mr Blackburn's Financial Crime and Compliance Change Program presented to and accepted to the Board on 24 May 2021; and

(b) Reports prepared by Mr Weeks which track Crown's progress against the remediation plan agreed with the Independent Liquor and Gaming Authority (NSW).

1.3.4 In addition, aspects of Crown's control framework and operations relevant to our work have been subject to external review and investigation by third parties who have direct access to Crown personnel, systems and exemption from the tipping off rules.[1] We have used the reports issued by the following advisers to inform our work:

(a) Deloitte's Phase 1 report dated 26 March 2021 in which Deloitte provides an independent assessment of the design and operation effectiveness of controls in respect of patron accounts (the **Deloitte Report**);[2]

(b) Promontory's Phase 1 report dated 24 May 2021 in which Promontory provides an independent assessment of Crown's AML vulnerability (the **Promontory Report**);[3] and

(c) Initialism's report dated April 2021 in relation to its review of Crown's Transaction Monitoring (**Initialism TM Report**).[4]

1.3.5 Our work has also been informed by:

(a) The report dated 1 February 2021 of the inquiry conducted by Patricia Bergin SC pursuant to section 143 of the Casino Control Act 1992 (NSW) (the **Bergin Inquiry** and the **Bergin Report**); and

(b) Consultation with Ms Rachel Waldren of Murray-Waldren Consulting, a subject matter expert in AML/CTF legislation and compliance.[5]

1.3.6 We have relied upon the documents sourced and reports prepared by others only where we are satisfied that the work undertaken by others is sufficient and appropriate to support their findings and the evidence they cite is not inconsistent with our findings or observations. All use of these reports is specifically referenced within this report.

[1] AML/CTF (Exemption Crown Entities) Instrument 202 (No 11) dated 14 April 2021

[2] DTT0005.0001.0038

[3] CRW.512.086.003

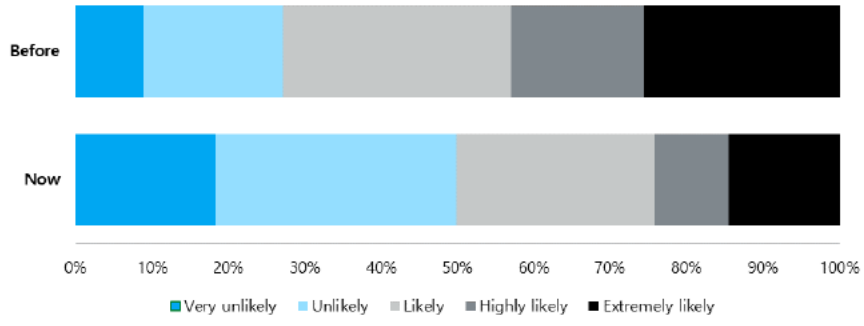
[4] INI.0004.0001.0172

[5] murraywaldren.com

1.4 Overall Findings and Observations

1.4.1 Table 2 below sets out our overall findings and observations derived from our investigations and analysis. Our findings and observations in relation to each area of the scope follow. All findings and observations are to be read in conjunction with this report in its entirety, including the scope of work (section 2.3) and limitations (section 2.6).

Table 2

	Overall Findings and Observations
1.	Crown's remediation of its approach to management of ML/TF risk and fulfilment of its obligations to deter, detect and report ML/TF activity is a work in progress and is far less advanced than could reasonably be expected of an entity which has been providing gaming services for some 30 years and subject to obligations to operate a risk based AML/CTF Program to mitigate and manage risk for some 15 years.
2.	Crown's journey towards a modern and effective AML/CTF regime appears to have been seeded in or about 2017[6] however little progress appears to have been made until around September/October 2020. At this time, the Bergin Inquiry was uncovering evidence of behaviours and transactions indicative of money laundering and Crown took steps to: ▪ Introduce several significant AML focussed policy and process changes; ▪ Initiate the recruitment of a senior leader to the position of Group Chief Compliance and Financial Crime Officer; a new role with direct reporting lines to both the Board and the Group CEO, taken up by Mr Blackburn from 24 February 2021; and ▪ Significantly expand the headcount in its AML related functions by some 40 FTE such that there were approximately 50 FTE by the end of May 2021. Our survey taken in June 2021 indicates that Crown employees are of the view that Crown has made progress. The chart below shows how survey respondents assessed the likelihood of money laundering happening at Crown now as compared to "before".[7] **Proportion of all respondents assessment of likelihood of ML occuring at Crown - Comparison between Before and Now**  *Source: McGrathNicol survey of Crown employees June 2021* As the chart shows in respect of money laundering at Crown Melbourne before COVID-19 and now: ▪ The proportion of respondents who consider it Highly or Extremely Likely has almost halved to 23%. ▪ The proportion of respondents who consider it Very Unlikely or Unlikely has doubled to almost 50%. ▪ Fewer, but still more than 10% of respondents consider that it remains Extremely Likely. The comments provided with these responses indicate there is a general view that there will always be money laundering at a Casino in particular because un-carded[8] activity below the $10,000 transaction threshold cannot be tracked and is not reported unless it observed to be suspicious.

[6] This date was mentioned by employees in focus groups and surveys and t coincides with the recruitment of Ms Louise Lane as Group General Manager AML

[7] "Before" was described as "pre-COVID" as a proxy for the time before the Bergin Inquiry, COVID impact on international clientele and the cessation of junkets

[8] Transactions with and play by persons who do not have a Crown Rewards card and can remain anonymous and where there is no obligation to report their transactions of less than $10,000

3. Mr Blackburn reviewed the status of Crown's AML functions and presented his assessment of the current state of what he describes as the financial crime and compliance eco-system to the Board on 24 May 2021. Mr Blackburn states that that "*Crown Group has significantly invested in its financial crime program over the last year and a half*"[9] and assesses the current state as at 31 May 2021, following that investment.
This places the significant investment and changes referred to as having occurred subsequent to:
- the appointment of Ms Bergin SC to conduct an inquiry pursuant to s143 of the Casino Control Act (1992) (NSW); and
- the introduction of several significant AML focussed policy and process changes which particularly target potential indicators of money laundering identified in the Bergin Inquiry.

4. Notwithstanding significant investment and the changes over the previous 18 months Mr Blackburn assesses the **overall current maturity of the financial crime program** (**FCP**) **at 31 May 2021 as "foundational**" with the majority of elements being "foundational" and some elements being "initial" or "transitioning to foundational".[10]

The attributes which result in Mr Blackburn's assessment of Crowns FCP as "foundational" and our comments as set out below lead to our view that if the FCP is foundational, it is only barely and recently so.

Attribute of "foundational"	**McGrathNicol view**
Having a compliant joint AML/CTF Program	An investigation of Crown's compliance with the AML/CTF Act and Rules is not within the scope of our engagement. However we observe that a prerequisite for the development of a compliant AML/CTF Program is a risk assessment so that the program can meet the requirements that it be risk-based and take into account the size, nature and complexity of the business as required by the Act and the Rules. We also note that: ▪ Mr Blackburn's FCCCP includes a plan to undertake an enterprise wide (ML/TF) risk assessment to be completed by December 2021. ▪ The prevailing joint AML/CTF Program (November 2020) does not refer to an underlying risk assessment and, as a result, the program presents as a restatement of the requirements of the Act and Rules and lacks the tailoring expected.[11] On this basis, we question whether Crown's Joint AML/CTF Program is compliant at this time.
Most processes documented	Policies and processes are documented but lack a clear hierarchy. This is an issue also being addressed in the FCCCP.
Foundational resources and capability in place	In May 2021 the personnel in AML/CTF functions numbered approximately 50 employees which we understand was an increase of more than 40 positions over the preceding 6 months. The FCCCP proposes recruitment for a further 50-60 positions to bring the team to a headcount of approximately 110. We would we agree that resources are foundational, but this state has only been achieved in very recent months.
Largely manual processes deployed	This assessment aligns with our observations and raises questions about the sustainability of the AML/CTF function.
Basic controls and systems are operating.	This assessment aligns with our review of controls, but we note that several significant controls have been introduced only in the last 6-8 months.

[9] Statement of Steven Blackburn to RCCOL 7 June 2021 CRW.998.001.0036

[10] Ibid paragraph 8 and CRW.512.081.1750

[11] This conclusion was reached in consultation with Ms Rachel Waldren, an AML/CTF compliance expert of Murray-Waldren Consulting www.murraywaldren.com

5.	The **Financial Crime & Compliance Change Program** is a roadmap for significant development and change in Crown's financial crime and compliance program over the period to December 2022. It was developed by Steven Blackburn, Chief Compliance and Financial Crime Officer (CCFCO) and approved by the board on 24 May 2021. Mr Blackburn is responsible for its implementation. By any measure it is an ambitious plan aiming to raise the maturity of the financial crime and compliance regime from "foundational" to "advanced" by December 2022. At the same time it is necessary if Crown is to comply with its obligations to have an AML/CTF Program which is risk based and commensurate with the size and complexity of the organisation, and ensure the management and operation of the casinos remains free from criminal influence or exploitation as envisaged by the Casino Control Act 1991 (Vic) (section 1(a)(i)). Over and above the $21.7 million costs involved in doubling the already expanded financial crime and compliance team, the plan calls for support and commitment, backed by funding, from across the business and from the board down to the casino floor. As Mr Blackburn states in his 24 May 2021 memo to the Board: *To be successful, each of the foregoing changes require the commitment, engagement and support of the whole organization and the Board, as well as committed funding for the longevity of the FC&C Change Program.* The risks to successful implementation are many; the critical risks are: funding, technology and people. ***Funding:*** Mr Blackburn joined Crown from National Australia Bank having sought and been given assurances by members of the Crown Board that he would have their backing to execute his mandate. The Board has approved his FCCCP and the $21.7 million per annum cost in terms of increased headcount. More funding will be required in regard to the demands of the FCCCP on other areas of the business; we are not aware that specific funding requests have been advanced in this regard. ***Technology:*** Mr Andre Ong, Group Chief Information Officer, leads a team of around 180 personnel in the IT team which is supplemented by contractors as required. Mr Ong who has been with Crown for approximately 7 years, describes his mandate as "to rationalise, centralise and uplift Crown's IT systems" of which he believes there are more than 300 of which 50-60 are business critical. He was consulted by Mr Blackburn in regard to the technology requirements of the FCCCP. Mr Ong is of the view that everyone, from the Board down understands the priority and he does not doubt that the necessary funding will be available, but as yet the projects involved are at a very preliminary stage and are not scoped or costed. ***People:*** Another key dependency is attracting skilled employees in significant numbers, absorbing them and having them quickly scale the learning curve (they are unlikely to bring casino experience) to deliver the many elements of the program by December 2022. To assist this, the FCCCP includes an uplift in salaries for the required positions to ensure they are market competitive. Mr Blackburn indicates that he recognises this challenge but is confident that market salaries and the opportunity for involvement in such a significant transformational project will be attractive to the talent he needs to supplement Crown's talent, including deep casino experience, which he advises he has found to be engaged and committed to the change. Equally, it is our assessment that some of this talent has already been stretched working on the change program in addition to the burdens of the various inquires, accordingly in addition to supplementing resources, strong leadership and human resource management will be necessary to keep the team focussed and energised over an 18 month period if the FCCCP is to succeed. It is our assessment that **it is likely that the FCCCP will give rise to a significant change** in Crown's understanding of and performance in AML/CTF over the ensuing 18 months. We say this because: ▪ We consider that Mr Blackburn has the capability, track record and standing to lead such an ambitious program. Further, he is not burdened by the history of Crown's past underperformance and has the "fresh eyes" advantage through having subject matter expertise honed in a different sector, which enables him to question practices and ideas which may not be considered open to question by those with only Crown or casino experience. ▪ The FCCCP he has developed is comprehensive and the areas of priority are apt. ▪ There is currently a rare window of opportunity to embed new processes and practices which may be challenging to customers, in an environment of little international patronage and lower patronage overall. Should Sydney Casino open, it too presents an opportunity to introduce practices and technology to bolster ML/TF resilience in a greenfield environment which can be replicated at other properties.

	▪ A number of significant control changes have already been implemented and appear to be effective. We note however that this assessment is made at a time when the casino is operating at low volumes and, moreover is subject to intense scrutiny which would have staff on high alert and would be keeping money launderers away. ▪ Our sense from the surveys we conducted, and the focus groups held was that: – Employees in the first line of defence are ready, willing and able to do what is asked of them when it comes to upholding the rules; but they rely on others to set them in accordance with Crown's values which include "*do the right thing*". – Employees in the AML and Compliance team have welcomed the additional resources and the priority being given to their work. They also reported having experienced an increased level of understanding and co-operation from the floor staff; they did not wish to imply that they not receive co-operation before, but they were of the view that changes and training have made their jobs easier now. – Overall employees had a real concern to get this right. For some this was expressed in the context of fear that the casino license, and therefore their jobs, are at risk; for others it was expressed in terms of recognising they have a rare window while there is increased funding and support and they can make real strides in what they see as purposeful work.

1.5 Findings and observations – specific scope areas

1.5.1 Our findings in relation to each area of our scope are summarised in Table 3 and should be read in conjunction with the analysis in the body of the report as referenced. All findings and observations are to be read in conjunction with this report in its entirety, including the scope of work (section 2.3) and limitations (section 2.6).

Table 3

	Scope area	Findings and observations	Report section
1.	Patron Accounts	Patrons are able to deposit money with Crown for the purpose of future gaming. There are currently 7 banks accounts available for this purpose; an AUD account for each of Melbourne and Perth Casino and 5 foreign currency accounts. The monies received from patrons into these bank accounts are swept into Crown's operational bank accounts on a daily basis. Accordingly, the bank account balance does not represent patrons' monies; this can only be ascertained from the DAB[12] Accounts. Patron's monies held are not held on trust. Crown does not pay interest on patrons' funds nor does it have prudential requirements as a bank would. This lack of governance over funds held on behalf of customers appears at odds with the holding of customer's monies in other sectors. Crown accounts for patrons' deposits in DAB accounts and Safekeeping (**SK**) accounts which are an internal record of deposits and withdrawals from the patron's funds. Both account categories operate under the same rules.	4.5
2.	Analysis of DAB & SK account balances	At 15 June 2021 Crown Melbourne Ltd held $47.1 million of patrons' monies within its bank accounts: ▪ $22 million in 2,438 DAB accounts. ▪ $25.1 million in 89 SK accounts. ▪ Only 11 patrons had balances in both a DAB and SK account; the balance held one or the other. ▪ The largest balances were $1.5 million in a DAB account and $7.1 million in a Safekeeping account. ▪ In DAB accounts the mean average balance was $9,011 and the median was $156 indicating a large number of small balances. ▪ In the SK accounts the mean average balance was $282,563 and the median was $4,126 indicating a large number of small balances; the higher mean average was influenced by a few balances in excess of $5 million. Parking of funds may be indicative of ML activity because it creates a temporal distance between the source and the use of the funds and in this way is a form of layering. An analysis of DAB/SK accounts with a balance in excess of $50,000 (96 accounts) revealed that: ▪ 30 DAB accounts haven't had a recorded transaction since 2019 with the highest balance of these accounts being $1,500,000. ▪ 45 SK accounts haven't had a recorded transaction since 2020 with the highest balance of these accounts being $7,079,089.	5.4

[12] An acronym for Deposit Account Balance, but used to refer to the account which is essentially a ledger run by Crown to account for monies deposited w th it by patrons.

	Scope area	Findings and observations	Report section
3.	Deloitte review of bank account transactions	Deloitte was engaged on 22 February 2021 to undertake, inter alia, a review of transactions through the bank accounts in which patrons deposit funds. The purpose of the engagement was: "*to assist you [Crown] in addressing specific suggestions made in the Bergin Report as part of a broader pathway to render Crown Sydney and Crown Resorts as a "suitable" Casino licensee*" According to its letter of engagement, Deloitte's Phase 2(ii) scope is limited to a review of the bank account transactions. In our view, it is necessary to consider the transactions in the bank accounts and also how they are reflected, and how the funds are subsequently transacted, within the DAB/SK accounts in order to gain a fulsome picture of what has transpired. It is likely that additional information including gaming records and Unusual Activity Report (**UAR**)/Suspicious Matter Report (**SMR**) mentions would be necessary to gain a full understanding of a patron's actions and whether they are indicative of ML. We would expect that this additional information will be incorporated into Deloitte's review as the work progresses. As at the date of this report, Deloitte had not completed or reported its Phase 2(ii) analysis of transactions in the patron bank accounts.	4.7
4.	Analysis of DAB/SK account transactions for Structuring	Our analysis of the transactions through the DAB/Safekeeping accounts for the period 1 July 2019 to 15 June 2021 applied the following test for identification of potential structuring: *two or more cash deposits in respect of a single patron below $10,000 that, when combined over a set period (24, 48, or 72 hours), totalled to be more than $10,000.* Our analysis found that: ▪ 1,914 individual transactions concerning 272 unique patrons met this criteria within the 72 hour window including: – 1,472 transactions by 174 patrons within a 48 hours window: – 908 transactions by 174 patrons in the 24 hour window. ▪ The most recent transactions for Melbourne occurred on 25 May 2021. ▪ The most recent transactions for Perth occurred on 16 June 2021. We caution that behaviours identified through this analysis may relate to genuine gaming behaviour; additional information including the gaming records, past and contemporaneous and the statement of funds declaration (if applicable) would add to an understanding of whether this behaviour was indicative of ML activity. We would recommend further investigation of these transactions.	5.5

	Scope area	Findings and observations	Report section
5.	Analysis of bank account transactions: Third party payments	Both Deloitte and McGrathNicol have performed analysis to test the operational effectiveness of the Third Party Payments policy. We have relied on Deloitte's analysis of the Crown bank accounts into which patron funds are deposited and the transaction data for those bank accounts provided by Deloitte on 23 June 2021. Deloitte analysed bank account data from December 2020 to February 2021; McGrathNicol analysed bank account and DAB/SK account data from 1 July 2019 to 22 February 2021 (bank data) and 15 June 2021 (BAB/SK data), with the following results: ▪ Deloitte identified 2 deficiencies between December 2020 and February 2021. ▪ McGrathNicol identified 1,041 instances across 168 patron accounts of apparent third-party deposits; this included: – 52 instances after the issue of the Executive Office Memo on 8 April 2020 which first prohibited third party payments; – one instance after the Executive Office Memo of 20 October 2021 which reiterated the policy and addressed frequently asked questions; and – no instances after the Return of Funds Policy was introduced on 4 January 2021. In our view, these results indicate a notable change in customer behaviour which improves Crown's ML risk profile, albeit it has occurred in a period of low activity. We do not have sufficient information to reconcile the outcome of our analysis with Deloitte's findings.	5.6
6.	Analysis of bank account transactions: Structuring	We searched the available bank data to identify transactions which are indicative of structuring being: ▪ Cash transactions ▪ <$10,000 Our analysis was limited to transactions where the bank account narrative included a reference to "cash", and we were able to identify the patron ID from the bank data. We found two identifiable cash transactions of <$10,000 and these were associated with different patron accounts and, accordingly, do not exhibit the characteristics of structuring. This finding is consistent with Deloitte's review of transactions in the period December 2020 to February 2021.[13]	5.7

[13] DTT.005.0001.0038 p 37 Table 3 and footnote

	Scope area	Findings and observations	Report section
7.	New Patron account controls	The new controls to Patron accounts policies and controls introduced by Crown from September 2020 onwards are: ▪ Prohibition on aggregation of deposits. ▪ No acceptance of third-party payments ▪ No acceptance of cash deposits direct to bank accounts (they can be made at the Cage). ▪ Manual monitoring of Crown bank accounts to which patrons make deposits. ▪ Return of funds for deposits of cash, from third parties and those which lack the details necessary to validate that they are the patron's funds. This includes Withdrawal of License (**WOL**) (to be on Crown gaming premises) provisions for repeated failure to comply with the rules. In combination with existing controls, it can reasonably be expected that these controls, if effectively implemented, will serve to prevent the ML activity identified in the Bergin report and be effective in deterring cash structuring and cuckoo smurfing activity because: [redacted] However, the documented controls have the hallmarks of having been implemented at speed and in an ad hoc manner. There is a lack of clarity as to how the various policy elements fit together, they are not underpinned by a contemporaneous risk assessment and there are deficiencies in the supporting guidance materials which pose a challenge to consistency of application and measurement of effectiveness of the controls.	6
8.	Operational effectiveness of Patron Account controls	Deloitte's review of the design and operational effectiveness and determined that: ▪ the controls would be effective if implemented; ▪ that they had been operationally implemented; but: – that there was risk to the sustainability of some controls, notably the manual monitoring of bank accounts when activity at the casino resumes post COVID-19; and – there is a need for further development of the documentation of transactions guidance for completion to enhance consistency and facilitate assurance processes. We consider Deloitte's review to have been appropriate and the conclusions reached were supported by the work performed and reported. We have not identified evidence which contradicts Deloitte's conclusions.[14] We agree with Deloitte's assessment that the implementation of the policies is immature, untested in levels of high activity and reliant on largely manual processes and, accordingly, the sustainability of the controls as trade resumes post COVID-19 is open to question. The evidence from the surveys and focus groups conducted in June 2021 is that employees have a high awareness of these controls and of their roles in implementing the controls as part of the effort to mitigate money laundering risk.	4.7 6

[14] With the exception that the timeline on page 13 at 3.2 of the Deloitte Report erroneously represents that the Third Party Transfers and Money Remitters Policy was introduced on 16 November 2019. The policy document CRL.742.006.0101 indicates it was issued on 16 November 2020.

	Scope area	Findings and observations	Report section
9.	Return of Funds policy	The Return of Funds Policy issued on 4 January 2021, brings together policies concerning non-acceptance of third party funds, funds from money remitters and companies and extends it to cash deposits and deposits which lack required identification references (name and patron account) and evidence that the funds have come from a matching personal account. [redacted] Deloitte's Phase 1 report indicates that it tested compliance with the return of funds policy on respect of a sample of 25 transactions (of a possible 69 transactions) involving a return of funds and found that the policy had been fully complied with. Our review of the minutes of the Person of Interest Committee from November 2020 to February 2021 indicate that 2 people have been subject to a withdrawal of licence pursuant to the Return of Funds policy (Third Party Payments).	6.5
10.	Transaction monitoring - manual	Crown introduced manual monitoring of its bank accounts by the AML Team on 16 November 2020 to identify transactions which contravene policies in respect of third party transactions, transactions which do not appear associated with gaming, cash deposits and those which exhibit structuring behaviour. Deloitte undertook a review of the manual review process over a sample of 2 weeks and found deficiencies in the processes which rendered it unclear whether transactions had been identified as unusual and how they had been dispositioned, although through walkthroughs and discussion it appears the review met its objectives. The sustainability of this manual review process as activity at the casinos resumes post COVID-19 is questionable. Bringing on the automated Sentinel system is critical to maintaining vigilance over activity in the bank accounts at more normal levels of trade, in the interim, the processes require further development to build in consistency and enable efficient review and assurance.	6.4

	Scope area	Findings and observations	Report section
11.	Transaction monitoring - Sentinel	The program to develop **Sentinel** as an automated solution to monitoring activities for AML/CTF risk, commenced in 2018 in recognition that the manual review was onerous and error prone. The decision to use a centralised analytics engine (Splunk) receiving data from numerous sources within the casino in a format that allows many data sources to be considered concurrently, pursuant to a suite of rules designed to trigger alerts when behaviours indicative of ML occur, positions Crown well to develop a complete automated transaction monitoring program. The quality and robustness of any analytics program is only as good as the data it receives. There are a number of risks associated with the current data inputs, particularly the manual and complicated nature of SYCO and the lack of transparent quality control processes associated with the ingestion of data from other platforms. Crown has identified 31 rules to run over the ingested data to trigger alerts for investigation. The rules have been developed from research both internal and external of money laundering typologies. On their face, the rules proposed are appropriately targeted to identify potential transactions which may be indicative of money laundering. They cover behaviours such as structuring (over multiple periods), third party transfers, IFTIs to/from high risk jurisdictions, buy-ins and cash outs which are not consistent with gaming records, increases in bet size, multiple cheques issued, large/unusual transactions and cash transactions (assessed in the context of customer risk and gaming record) and significant losses. Subject to effective implementation, they are likely to enable detection of a broad range of potentially suspicious activity and certainly will be more efficient and likely more effective than the current manual processes, particularly when casino trade resumes. Of the 31 proposed rules, 18 are currently deployed, four rules are to be merged with other rules in phase 2 and nine rules will be deployed in phase 3. The timing of the phases is dependent on the progress of refining the phase 1 deployment. Sentinel has only recently been implemented and is effectively in a trial phase where issues of data quality on ingestion are being ironed out and the effectiveness and calibration of the alert rules is under review. The lack of operational data from Melbourne Casino has hindered the ongoing development of processes and rules. Crown's joint AML/CTF Program Part A, section 6, sets out the parameters for the Sentinel rules and processes to be undertaken in relation to alerts it triggers. The automated process ends with the Sentinel alert being raised and from there the process to convert alerts into investigations and recording of the disposition of the matter reverts to non-automated workflow processes using spreadsheets, emails and Teams tasks.	7.2

	Scope area	Findings and observations	Report section
12.	Know Your customer	The FCCCP identifies 9 elements of a program to uplift Crown's KYC regime. The nature of and need for the proposed changes suggests: ▪ Under-investment in information technology to enable instant verification of identification presented – to be addressed by October 2021 for high risk customers; ▪ Failure to comply with AML/CTF Rules through not undertaking a risk-based approach in mitigating the risks associated with customers and their jurisdictions – to be met by undertaking such a risk assessment by December 2021; and ▪ Complacency in not collecting basic KYC information from customers such as occupation. Recent improvements which have been made include: ▪ The Significant Player Review policy dated 12 March 2021 – Pursuant to this policy increasing levels of review and requests for KYC data are required from customers based on the level of their gaming activity. – Non-compliance with information requests or non-acceptable responses is grounds for banning. – By 21 May 2021, the review had been completed for 1,320 top customers of Melbourne Casino and 198 withdrawal of licenses had been issue. ▪ The Source of Funds policy issued in December 2020 – This policy requires customers to complete a Source of Funds declaration to explain the source of the funds they have presented for buy-in once they have presented cash which exceeds $25,000 on any calendar day. – This is in addition to a Threshold Transaction Report and, if applicable an Unusual Activity Report. – Failure to complete a Source of Funds declaration will trigger an Unusual Activity Report and the cash will not be accepted. – Implausible or incomplete information on a Source of Funds declaration will be escalated by the cashier to the cage manager and the transaction will not proceed. Feedback from employees through the focus groups is that 2 out of 3 cash transactions (which meet the threshold) do not proceed because of this policy; they report that customers prefer to walk away.	8.5

13.	Money laundering "On the floor"	The interviews, focus groups and surveys conducted by McGrathNicol provided evidence that employees are generally of the view that money laundering on the casino floor cannot be completely eliminated. In particular, they cite the threshold limit of $10,000 and the ability for customers to play un-carded as providing an open opportunity for money laundering. We have considered the vulnerability of Crown to money laundering OTF with reference to the Promontory Report, Crown's response to the Promontory Report, the FCCCP and the information gathered through our interviews, surveys and focus groups. The controls to mitigate money laundering OTF may be considered as: ▪ Controls relating to customers; ▪ Controls relating to cash; and ▪ Controls relating to employees. *Customer and cash controls* Crown has many controls which are applied to disrupt potential money laundering primarily through: ▪ Minimising opportunity for anonymity and maximising collection of customer information, for example: – Crown Rewards Card required for entry to all VIP rooms; – Since 30 June 2021 ID to be provided for all cash transactions in excess of $4,999; and – Statement of Funds required for cash presented which exceeds $25,000 on any day. ▪ Limitations on activities to undermine the ability to launder money, for example: – imits on cash transactions which vary as between where the patron is gaming; – speed limits on chip and ticket dispensing machines; – ban on requests for particular dealers; and – [redacted] ▪ Surveillance and denial of entry to people who have a record of criminal behaviour or dishonesty or have breached or are unprepared to comply with Crown's rules. The FCCCP include actions to strengthen Crown's capacity to deter, detect and report OTF money laundering. These actions include: ▪ Digital verification of identification – for all new customers then for existing customers, with suspension as the alternative to undertaking digital verification. ▪ Printing customer names on TITOs and making them non-transferable. ▪ Limiting un-carded play on EGMs and eTGs. ▪ Recording cash buy-ins. ▪ Improved data via dashboards to the Cage to assist in recognition of suspect activity. We note that a number of the FCCCP proposals have a technology component and are framed in terms of ascertaining feasibility, rather than a commitment to proceed. *Employee controls – Vetting and training* Crown has policies and processes which mitigate the risk that an employee will be corrupt or corrupted such that they will participate in or turn a blind eye to behaviours indicative of financial crime. These include: ▪ Vetting of all candidates prior to employment to ensure they do not have a history of financial crime or any indications they may be susceptible to carrying out actions in breach of Crown's policies. This is in addition to the processes undertaken by the VCGLR before it grants a Special Casino Employee Licence which all employees involved in the delivery of designated services or in positions of management must have before working at Crown. ▪ Ongoing vetting of current Crown employees using the Dow Jones Risk and Compliance product to screen employees on a daily basis to identify any	10

	Scope area	Findings and observations	Report section
		adverse media or risk factors, for example court appearances or inappropriate associations which may be of concern. ▪ Conduct of analytics over employee's social media, address and emergency contacts to assist in detecting potential collusion with casino patrons or high-risk persons. ▪ Pro-active and reactive surveillance of employees and review of gaming data to identify any unusual patterns, for example patrons always or only gaming with the same croupier. AML/CTF training is an important aspect in ensuring that Crown employees understand the risk of money laundering and the ways in which it can be carried out. The results of the surveys and focus groups we undertook indicate that generally: ▪ OTF employees have a good understanding of the different methods of money laundering that may occur and they believe they have the knowledge they need to recognise when something is not right; ▪ They are aware of what is expected of them should they see behaviours which are to their mind unusual; ▪ They appeared to understand the obligation to report, via a UAR, what they see as an individual responsibility – if they see it and think it is unusual they report it, irrespective of whether their colleague has the same view; ▪ They are aware of the UAR process and what is required; and ▪ They receive both formal and informal training on AML/CTF. In both surveys and focus groups employees remarked on the increased and strong focus on AML and the expectations on them to assist Crown to fulfil its obligations. The FCCCP include actions to strengthen Crown's capacity to deter, detect and report OTF money laundering. Actions include the further development and deployment of AML training to reposition the emphasis towards outcome based learning – "*we are doing these things to protect the vulnerable from the consequences of enabled money laundering" rather than "we are doing these things so we comply with regulation*". In our assessment, Crown is on a path involving a range of individual measures which collectively, if implemented as proposed, will make the casino an increasingly unattractive option for would be money launderers. Some of the employees in the focus groups indicated it was becoming increasingly unattractive for regular customers also. The reduction of the un-carded play limit to $4,999 is a significant move which will restrict the activities of those previously undetected and undetectable launderers.	

2 Background, engagement and scope of work

2.1 Background

2.1.1 McGrathNicol Advisory (**McGrathNicol**) has been engaged to provide forensic investigation services to assist the Royal Commission into the Casino Operator and Licence (**RCCOL**) to undertake its inquiry in accordance with its terms of reference dated as gazetted on 22 February 2022.

2.1.2 The RCCOL was called as a result of the findings of the New South Wales Independent Liquor and Gaming Authority Inquiry into, inter alia, the suitability of Crown Sydney Gaming Pty Ltd (**Crown Sydney**), a subsidiary of Crown Resorts Ltd (**Crown Resorts**), to hold a restricted gaming license (**Bergin Inquiry**).

2.1.3 The key findings and conclusions of the Bergin Inquiry were that:

(a) Crown Sydney was not a suitable person to continue to give effect to the restricted gaming license;

(b) Crown Resorts was not a suitable person to be a close associate of the person holding the restricted gaming license;

(c) That Crown Resorts:

(i) Facilitated money laundering;

(ii) Disregarded the welfare of its China-based staff by pursuing an aggressive sales policy and failing to escalate risks through appropriate risk management structures;

(iii) Entered into or continued commercial arrangements with junket operators with links to organised crime; and

(iv) Some conduct canvassed by the Bergin Inquiry related to the Melbourne Casino (**the Casino**) operated by Crown Melbourne Limited (**CML**).

(d) The Terms of Reference of the RCCOL require inquiry into and reporting of a range of matters including, but not limited to:

(i) The suitability of CML to continue to hold the Victorian casino licence;

(ii) Whether Crown Resorts and other associates of CML and Crown Resorts are Suitable Associates of CML under the Act;

(iii) If applicable, what would be required for CML, Crown Resorts or existing associates to become Suitable Associates;

(iv) CML's compliance with the requirements of the Act and certain contracts referred to within the Act; and

(v) Whether it is in the public's interest for Crown to hold the casino licence and if not, what is required to redress that situation.

2.1.4 Key appointees of the RCCOL are:

(a) Raymond Finkelstein QC - Commissioner and Chairperson of the Royal Commission (**the Commissioner**);

(b) Corrs Chambers Westgarth (**Corrs, Solicitors Assisting**) - solicitors to the Royal Commission with a team led by Abby Gill, Craig Phillips and John Tuck; and

(c) Adrian Finanzio SC, Penny Neskovcin QC, Geoff Kozminsky and Meg O'Sullivan – each Counsel Assisting RCCOL (**Counsel Assisting**).

2.2 Engagement of McGrathNicol

2.2.1 McGrathNicol was engaged by the State of Victoria pursuant to the terms of a Master Supply Agreement[15] under a purchase order dated 31 March 2021 issued to provide services referred to in the McGrathNicol proposal dated 24 March 2021.

[15] For the provision of Professional Advisory Services dates 1 September 2020

2.3 Scope

2.3.1 The scope of McGrathNicol's work concerns whether CML allows the Melbourne Casino to facilitate money laundering as a means of informing the Commission in relation to Crown's suitability to hold the licence to operate the Melbourne Casino.

2.3.2 By agreement between the Solicitors Assisting and Crown, the scope has been addressed by undertaking the following investigative procedures:

(a) Desktop review of relevant documents obtained from various parties under notices to produce issued by the RCCOL and provided to McGrathNicol by the Solicitors Assisting the RCCOL;

(b) Guided tours of Melbourne Casino;

(c) Interviews with a number of senior employees;

(d) Issue of questionnaires which were completed by certain senior and management employees;

(e) Survey of significant number of floor staff;

(f) Survey of second line of defence staff;

(g) Focus group discussions with small groups of Crown Casino floor staff; and

(h) Focus group discussion with a small group of Crown employees with roles involving AML control oversight.

2.3.3 The agreed scope is set out in Appendix A and summarised in Table 4.

Table 4 Summary of scope items with reference within this report

Scope element	Report Reference
Indications of money laundering in Patron Bank Accounts ▪ Background to Riverbank and Southbank account findings in Bergin Report ▪ Review of Deloitte's Project Libby – scope and reports to date ▪ Undertake work to identify indications of money laundering in Patron Bank Accounts post closure of Riverbank and Southbank accounts in 2009	**4 and 5**
Review new AML (patron account) controls ▪ Review Deloitte assessment of controls ▪ Review controls implemented ▪ Gather information on impact of new controls to date ▪ Assess risks to successful implementation ▪ Assess sustainability of controls	**6**
Transaction Monitoring Processes ▪ Review purpose and progress of implementation of Sentinel to identify money laundering typologies within available data sets (primarily bank accounts and gaming data) ▪ Consider effectiveness and sustainability of current manual processes	**7**
Identify and review KYC processes embodied in AML/CTF Program approved by board in October 2020 ▪ Consider policies and processes used for identification and for identification of risks ▪ Criteria for assessment of customer risk ▪ Due diligence, ongoing due diligence and enhanced due diligence processes ▪ Assess effectiveness and risks to effectiveness and sustainability	**8.2**
Review and assess the Financial Crime and Compliance Change Program (FCCCP) prepared by Steven Blackburn and approved by the Board on 24 May 2021. Consider: ▪ Key elements and alignment with McGrathNicol findings and observations ▪ Implementation risks and effect on timing ▪ Priorities and dependencies within the FCCCP	**9**
Money laundering "on the floor" (OTF) ▪ Identify and assess the impact of controls upon known ML typologies which may occur on the floor ▪ Review measures in place to assure employee integrity on employment and on an ongoing basis	**10**

2.4 Work performed

2.4.1 Table 5 summarises the various enquiries undertaken in addition to document review and research.

Table 5 Enquires undertaken

Interviews*:	Each of between 1 and 2 hours duration	
Date	**Interviewee(s)**	**Title**
3 June	[redacted]	
3 June	Steven Blackburn	Group Chief Compliance & Financial Crimes Officer
3 June	[redacted]	[redacted]
8 June	[redacted]	[redacted]
24 June	Andre Ong	Group Chief Information Officer
Group interview - Patron / DAB accounts		
2 June	[redacted]	[redacted]
Group interview - Employee risks		
7 June	[redacted]	[redacted]
Group interview - Sentinel		
8 June	[redacted]	[redacted]
Safekeeping accounts group interview		
28 June	[redacted]	[redacted]

Questionnaires			
Participant	**Title**	**Date issued**	**Response date**
Craig Walsh	Executive Director Security and Surveillance	28 May 2021	10 June 2021
Michelle Fielding	Executive General Manager Regulatory and Compliance	31 May 2021	6 June 2021
[redacted]		31 May 2021	7 June 2021
Anne Siegers	Chief Risk Officer	31 May 2021	9 June 2021
Jessica Ottner	Group General Manager - Internal Audit	31 May 2021	8 June 2021

Surveys					
	Participants	**Issued**	**Responses**	**Date opened**	**Date closed**
1	Front line (OTF) staff	1,399	337	25 June 2021	8 June 2021
2	Second line (AML/Compliance) staff	48	38	25 June 2021	8 June 2021

Focus Groups			
	Participants	**No. Participants**	Date held
1	Casino floor employees	7	24 June 2021
2	Casino floor employees	8	24 June 2021
3	AML/Internal audit employees	9	25 June 2021

** additional McGrathNicol staff and an Allens representative also attended*

2.5 Information relied upon

2.5.1 A number of documents were provided to McGrathNicol by the Solicitors Assisting.

2.5.2 Specific documents referred to are identified in footnotes.

2.5.3 In addition, aspects of Crown's control framework and operations relevant to our work have been subject to external review and investigation by third parties who have direct access to Crown personnel, systems and exemption from the tipping off rules.[16] We have used the reports issued by the following advisers to inform our work:

(a) Deloitte's Phase 1 report dated 26 March 2021 in which Deloitte provides an independent assessment of the design and operation effectiveness of controls in respect of patron accounts[17] (the **Deloitte Report**).

(b) Promontory's Phase 1 report dated 24 May 2021 in which Promontory provides an independent assessment of Crown's AML vulnerability[18] (the **Promontory Report**).

(c) Initialism's report dated April 2021 in relation to its review of Crown's Transaction Monitoring[19] (**Initialism TM Report**).

2.5.4 Our work has also been informed by:

(a) the report dated 1 February 2021 of the inquiry conducted by Patricia Bergin SC pursuant to section 143 of the Casino Control Act 1992 (NSW) (the **Bergin Report**); and

(b) consultation with Ms Rachel Waldren of Murray-Waldren Consulting, a subject matter expert in AML/CTF legislation and compliance.[20]

2.5.5 We have relied upon the documents sourced and reports prepared by others only where we are satisfied that the work undertaken by others is sufficient and appropriate to support the findings and the evidence they cite is not inconsistent with our findings or observations. All use of these reports is specifically referenced within this report.

2.6 Limitations and disclaimer

2.6.1 McGrathNicol addressed the scope as described in section 2 3 of this report. We did not have unfettered access to Crown premises or personnel. We did not have access to and accordingly have not reviewed all information

[16] AML/CTF (Exemption Crown Ent ties) Instrument 2010 (No11) dated 14 April 2021

[17] DTT0005.0001.0038

[18] CRW.512.086.003

[19] INI.0004.0001.0172

[20] murraywaldren.com

which may have been provided to the Commission by Crown or other parties. The Solicitors Assisting provided McGrathNicol with access to documents obtained by the Commission which they considered relevant to the scope; these were supplemented by documents requested by us which were either provided by the Solicitors Assisting (where they had been produced) or were obtained for us under notices to produce.

2.6.2 Where we have reproduced the word of others, for example from survey responses or questionnaires, we have not made any corrections to spelling, grammar or punctuation.

2.6.3 McGrathNicol is not exempted from the tipping off rules under the AML/CTF (Exemption-Crown Entities) Instrument 2021 (No.11); we understand that this precluded unfettered on-site access. In addition, we have not been privy to information regarding reports which may have been submitted to AUSTRAC or otherwise informs as to suspicions of money laundering. Accordingly, to the extent we have identified incidences which may be indicative of money laundering activity, we are unable to comment as to whether such incidences have been identified or reported by Crown.

2.6.4 This report has been prepared in accordance with the terms of the engagement as described in sections 2.1 to 2.3 above.

2.6.5 This report has been prepared for the Solicitors assisting the RCCOL. It should not be disclosed to any other party, without our consent in writing. It may not otherwise be reproduced in whole or in part or supplied to any other party, without our consent in writing.

2.6.6 Please note that in accordance with our firm's policy, we are obliged to advise that neither the firm nor any member or employee of the firm undertakes responsibility in any way whatsoever to any person or organisation other than the Solicitors assisting the RCCOL in respect of the information set out in this report, including any errors, omissions or negligence however caused.

2.6.7 The information contained in this report has been prepared on the basis of the work undertaken as described in section 2.3.2 and 2.4 and the documents referred to throughout this report.

2.6.8 We have not carried out an audit, nor have we verified any of the information provided to us, except where expressly stated.

2.6.9 The information in this report may not include all possible or relevant information in relation to the matter we have been instructed to investigate. Whilst every effort has been made to ensure the information contained in this report is accurate, McGrathNicol accepts no responsibility if the information ultimately turns out to be incorrect or not applicable. We note that, in issuing this report, McGrathNicol is not certifying that we have identified all relevant events and information. We have sought to identify all significant events from the information provided but provide no assurance that all such significant events and information have been identified.

3 About money laundering in casinos

3.1 Money laundering in Australia and globally

3.1.1 Money laundering is the process of legitimising the proceeds of criminal activities so that the criminal origin of the funds cannot be traced. The United Nations estimates that money laundering of around $1.6 trillion occurs each year, which is around 2.7% of global GDP.[21] Australian annual casino gambling turnover is over $26.2 billion (2018-2019 figure)[22] [23] and many of the transactions involve the use of cash. This high transaction volume and cash environment makes casinos attractive for money launderers.

3.1.2 For context, in the sections which follow, we provide a high level overview of money laundering, the typologies which are relevant to the focus of this report, the general techniques involved in an anti-money laundering control regime and an overview of the legislative and regulatory obligations of Crown in respect of the Melbourne Casino.

3.2 Money laundering phases

3.2.1 Money laundering is typically considered to involve three distinct stages:[24] [25]

(a) *Placement* is the initial stage where the launderer moves the illicit funds into a legitimate financial system such as a casino. At a casino, placement may occur when, for example, illicit cash is:

(i) deposited into a patrons casino account or in repayment of a casino debt

(ii) exchanged for alternative instruments of value including:

- buy in of chips at a buy in desk
- buy in of chips on a gaming table
- purchase of a table voucher at the Cage
- purchase of a gaming machine ticket at the Cage
- purchase of chips from a chip dispensing machine (**CDM**)
- purchase of winning ticket in ticket out voucher (**TITO**) from another patron at a premium

(iii) fed into electronic table games (**eTG**s)

(iv) fed into electronic gaming machines (**EGM**s)

(v) exchanged for clean cash through the Cage or Ticket Redemption Terminal (**TRT**)

(b) *Layering* is where the launderer tries to conceal the origin of the funds by undertaking transactions or activities which aim to obfuscate their source, by multiple transition of forms of value and otherwise separating the funds from their source, including by the elapse of time. Examples of layering behaviour involving the casino may include:

(i) Funds being parked in casino accounts.

(ii) Chips removed from the casino and not used for gaming immediately and later appearing to be cashed out,

(iii) Use of international funds transfers to patron accounts create geographic distance between the funds and their source.

---

[21] Un ted Nations article ent tled *Tax abuse, money laundering and corruption plague global finance* dated 24 September 2020 https://www.un.org/development/desa/en/news/financing/facti-interim-report.html

[22] https://www.qgso.qld.gov.au/issues/2646/australian-gambling-statistics-36th-edn-1993-94-2018-19.pdf

[23] Includes actual turnover for keno and gaming machines and handle (amount of money exchanged for gaming chips at gaming tables) for table games

[24] Un ted Nations Office on Drugs and Crime website https://www.unodc.org/unodc/en/money-laundering/overview.html

[25] https://www.moneylaundering.ca/public/law/3_stages_ML.php, https://calert.info/details.php?id=1239

(c) *Integration* is the stage where the funds are returned to the launderer in a form where it is difficult to distinguish them from legitimate funds. Examples of integration achieved through casino transactions include:

(i) Cashing into chips or EGM credits and cashing out with minimal play;

(ii) Intentional losing in peer to peer games such as poker where illicit funds are lost to the benefit of a single player who then cashes out the winnings for a cheque or bank transfer;

(iii) Playing both sides of a near even money bet (e.g. black and red or odds and evens on roulette) such that monies lost approximate monies won which transforms the funds to winnings claimed by cheque or bank transfer; or

(iv) Cashing out TITOs, Crown Reward Credits or chips acquired with low denomination notes for high denomination notes.

3.3 Money laundering in casinos

3.3.1 The scope of this report is to consider the exposure of Melbourne Casino to money laundering which may occur through transactions in patron accounts and activities in all areas of the Crown Casino complex which are licensed for the conduct of gaming activities (**Gaming floor**).

3.3.2 There are numerous money laundering typologies and they evolve over time. Regulatory bodies (such as AUSTRAC) publish yearly reports on money laundering typologies and examples of 'red flags' which are relevant to casinos.[26] Crown has also published a list of 'Red flag Indicators Examples' which they have made available to their employees, which includes examples of behaviours which may indicate money laundering.[27]

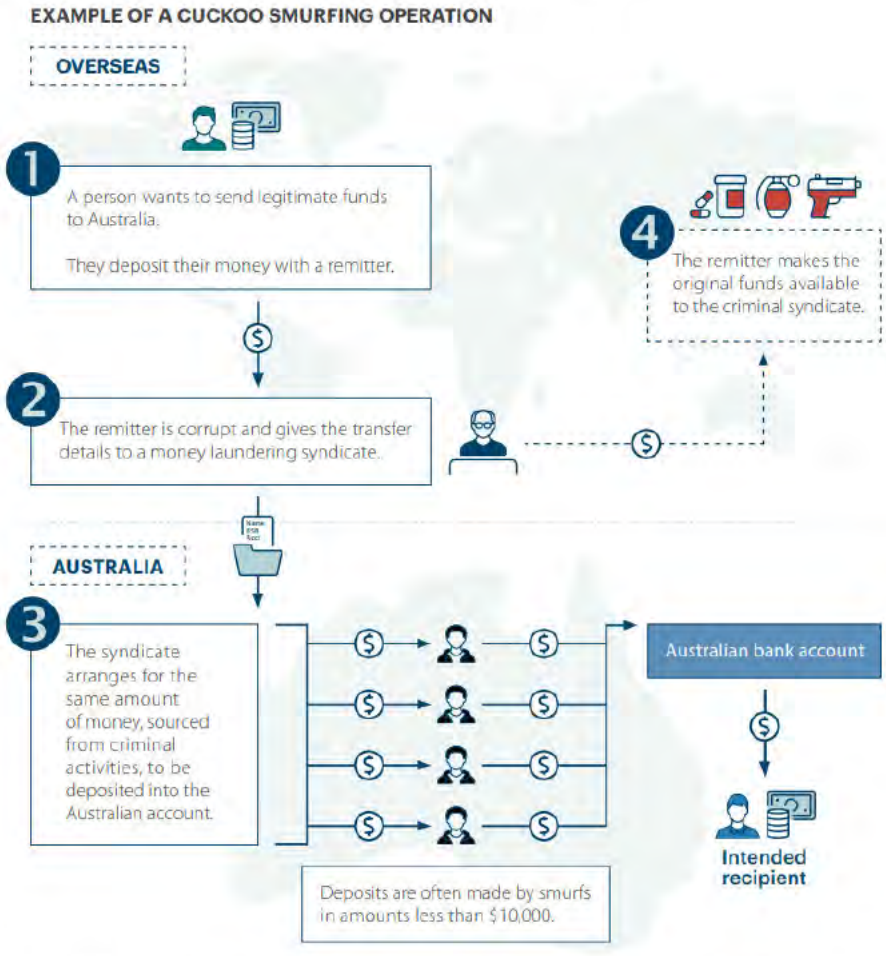
3.3.3 A common money laundering typology is cuckoo smurfing (refer to Figure 1 below), which involves corrupt money remitters and the exploitation of legitimate bank accounts of customers who are waiting to receive legitimate funds. The criminals transfer the funds that the legitimate customer is expecting to receive into their account and these customers unknowingly receive proceeds of crime. It often also involves 'structuring' which AUSTRAC describes as *"the deliberate division of a large amount of cash into a number of smaller deposits to avoid a single larger transaction and fall below the reporting threshold".*[28]

[26] https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/typologies-paper-austrac-money-laundering-and-terrorism-financing-indicators

[27] Crown AML document entitled *Red Flag Indicator Examples*, reference INI.0003.0001.0214

[28] https://www.austrac.gov.au/s tes/default/files/2021-06/AUSTRAC_FCG_CuckooSmurfing_web.pdf

Figure 1 AUSTRAC example of a cuckoo smurfing operation



3.3.4 In Table 6 we set out the red flag indicators identified by AUSTRAC[29] and Crown to which Crown may have exposure in relation to its patron accounts or OTF as relevant to the scope of our review.

Table 6 Money Laundering Typologies identified by AUSTRAC and Crown

	Typology	Affects Patron accounts / OTF
1	Bill stuffing (in large amounts under $9,999), where a patron goes to various gaming machines or eTGs, inserts cash in the bill acceptors and collects the ticket in ticket out (**TITO**), partakes in nominal or no gaming activity and then cashes the TITO out at the Cage.	OTF
2	Purchasing and cashing out casino chips with no gaming activity.	OTF
3	Deposit of gambling proceeds into a foreign bank account.	OTF
4	Frequent deposits of winning gambling cheques followed by immediate withdrawal of funds in cash.	OTF
5	Frequently playing games with low returns but with higher chances of winning.	OTF
6	Transfers from company accounts to private betting accounts.	Patron accounts
7	Use of third parties to purchase gaming chips.	OTF
8	Multiple chip cash-outs on the same day.	OTF
9	Multiple transactions of a similar nature on the same day in different locations.	Patron accounts

[29] https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/typologies-paper-austrac-money-laundering-and-terrorism-financing-indicators

	Typology	Affects Patron accounts / OTF
10	Unusually large cash transactions.	OTF
11	Transactions structured to avoid customer identification or reporting thresholds, where transactions are deliberately split into smaller amounts to avoid threshold transaction reporting to AUSTRAC e.g. structuring chip cash-outs.	OTF
12	Patron altering or cancelling a transaction to avoid reporting requirement.	OTF
13	Unknown source of chips.	OTF
14	Collusion between two or more patrons, such as one acting on behalf of the other.	OTF
15	Doubts around the plausibility of a customer's Source of Funds or Source of Wealth.	OTF
16	Potential loan sharking (lending money or chips and charging interest).	OTF
17	Identification or verification discrepancies, or the customer refuses to provide information.	OTF
18	Intentional losses or ambivalence to incurring losses, where the customer may be gambling with illegal funds and sees the losses as the cost of laundering money.	OTF
19	Customer frequently purchases chips, engages in minimal or no gaming activity, and is observed leaving the casino with the chips (chip walking).	OTF

3.4 Anti-money laundering

3.4.1 Anti-money laundering techniques aim to disrupt the placement/layering/integration flow and at a casino are generally centred around:

(a) Knowing your customer – a process of gathering intelligence on customers so that the casino knows with whom it is dealing and can:

(i) assess transactions by individuals as unusual or suspicious in the context of that knowledge; and

(ii) ensure persons who present a high risk of criminal infiltration are excluded from the premises.

(b) Cash controls – limiting the cash entering into and out of the casino.

(c) Controlling non-cash funds movements – receiving and paying funds only and directly to the patron engaged in gaming.

(d) Transaction monitoring which includes:

(i) capturing data on all casino transactions and reviewing for transactions or patterns for behaviour which are unusual and potentially indicative of money laundering typologies; and

(ii) observing behaviours and ensuring transactions are consistent with observations or records of actual behaviour.

(e) Surveillance and observation to identify unusual behaviours.

3.5 Legislative and regulatory obligations

3.5.1 An underlying premise of legislation and regulation of casinos is that casinos pose an inherently high risk of criminal activity and influence. Unchecked, casinos will be used to facilitate money laundering by both individual criminals and those involved in organised crime.

Casino Control Act 1991 and other State legislation

3.5.2 Melbourne Casino is licensed to operate under the Casino Control Act 1991 (**Casino Control Act**) which recognises this risk in its purposes in section 1:

(a) To establish a system for the licensing, supervision and control of casinos with the aims of:

(i) Ensuring that the management and operation of casinos remain free from criminal influence or exploitation…

(b) To provide for actions that may be taken by the Chief Commissioner of Police with the aim of ensuring that the casino complex remains free from criminal influence or exploitation

3.5.3 The Casino is also subject to various other Victorian legislation and regulation concerning liquor licensing, responsible gambling, gambling regulation.

3.5.4 The Victorian Commission for Gaming and Liquor Licensing (**VCGLR**) is the independent statutory body responsible for regulating gambling and liquor industries in Victoria.

Anti-money Laundering and Counter Terrorism Financing Act

3.5.5 Gambling services are designated services[30] under the Federal Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (**AML/CTF Act**) and the Anti-Money Laundering and Counter-Terrorism Financing Rules (**AML/CTF Rules**). The AML/CTF Act and rules aim to prevent money laundering and the financing of terrorism by imposing a number of obligations on "reporting entities" which are businesses which provide "designated services".[31] AUSTRAC regulates compliance with the AML/CTF Act and Rules.

3.5.6 A key obligation of Crown under the AML/CTF Act is to have an AML/CTF Program specifying how the reporting entities comply with AML/CTF legislation.[32] Crown has a joint program which covers its designated business group (**DBG**) which includes all entities in the group which provide designated services.

3.5.7 An AML/CTF Program is to be risk based so that it addresses the money laundering and terrorism financing risks the business reasonably faces. Policies, procedures and controls to identify, mitigate and manage those risks are to be developed and document.

3.5.8 Accordingly, a necessary precursor to a compliant AML/CTF program is an ML/TF risk assessment of the likely level of risk of the designated services being used for money laundering, based on its size, nature and complexity, taking into account:

(a) who the customers are;

(b) the services provided;

(c) how the services are provided; and

(d) the foreign jurisdictions dealt with (as applicable).

3.5.9 An AML/CTF Program has two parts:

(a) Part A addresses the processes and procedures employed to identify, mitigate and manage the money laundering and terrorism financing risks reasonably faced.

(b) Part B addresses the procedures for identifying customers and verifying their identity (KYC) as well as enhanced customer due diligence (**ECDD**) which requires documentation of the actions taken when the ML/TF risk is high[33]. Ongoing customer due diligence is also required to ensure the information they have about customers and processes for ECDD and transaction monitoring is up to date.[34]

3.5.10 Under the AML/CTF legislation there are several primary reporting obligations:

(a) SMRs to AUSTRAC which are to be submitted when it is suspected that a person or transaction is linked to a crime:

(i) within 24 hours if the suspicious activity is related to terrorism financing; or

(ii) within 3 business days if the suspicious activity is related to money laundering.[35]

---

[30] Table 3 s6 AML/CTF Act

[31] https://www.oaic.gov.au/privacy/other-legislation/anti-money-laundering/

[32] https://www.austrac.gov.au/business/how-comply-guidance-and-resources/amlctf-programs/amlctf-programs-overview

[33] https://www.austrac.gov.au/business/how-comply-and-report-guidance-and-resources/amlctf-programs/enhanced-customer-due-diligence-ecdd-program

[34] https://www.austrac.gov.au/business/how-comply-and-report-guidance-and-resources/customer-identification-and-verification/customer-identification-and-due-diligence-overview

[35] https://www.austrac.gov.au/business/how-comply-guidance-and-resources/reporting/suspicious-matter-reports-smr

(b) Threshold Transaction Reports (**TTRs**) for transactions of A$10,000 or more in cash; and

(c) International Funds Transfer Instruction reports (**IFTIs**) for transfers of funds of any value into or out of Australia (both due within 10 business days).

4 Indications of money laundering in Patron Bank Accounts

4.1 The nature and purpose of Patron Bank Accounts

4.1.1 Crown offers patrons the facility to deposit money with Crown for the purposes of future gaming.

4.1.2 In this report we have used the term **Patron Account** to describe those bank accounts owned by Crown into which patron funds are deposited, and **DAB Account** or Safekeeping (**SK**) account to describe the accounting for the funds attributable to a patron.

4.1.3 The DAB Account and the SK account operate in the same manner.

4.1.4 Crown provides patrons with details of bank accounts to which monies can be deposited. When the patron wishes to access those funds for gaming, they present themselves at the Cage with evidence of their deposit. Cage staff verify the deposit and the patron is provided with chips or other gaming tender and an entry is made to the DAB/SK account to reflect the withdrawal.

4.2 Allegations and Bergin's findings in relation to Southbank and Riverbank accounts

4.2.1 The Bergin Report cites as a reason for undertaking the Bergin Inquiry, certain media allegations that Crown "*facilitated money laundering or turned a blind eye to such activity in the Southbank Investments Pty Ltd (**Southbank**) and Riverbank Investments Pty Ltd (**Riverbank**) accounts*".[36]

4.2.2 The media allegations appeared in an article entitled '*Crown's firms used to launder drug funds'* published in *The Sydney Morning Herald* on 5 August 2019 and *The Age* on 6 August 2019 (the **Media Allegations**). Allegations in the article included:

(a) Drug traffickers and money launderers had used the Southbank and Riverbank accounts to deposit suspected proceeds of crime between 2012 and 2016.[37]

(b) "One source said that federal police believed the two Crown companies were used by criminal entities because they believe that the money they deposited into them would not be closely scrutinised".[38]

4.2.3 The allegation that Crown facilitated money laundering was established by the Bergin Inquiry[39], while the allegation that Crown "turned a blind eye" to money laundering was not.

4.2.4 It is apparent from the Bergin Report that:

(a) Crown did not consider Southbank and Riverbank to be reporting entities under the AML/CTF Act and accordingly they were not subject to the same review as those entities that were identified as reporting entities.[40]

(b) Some Cage staff aggregated numerous deposits made to the credit of a single patron account into one entry in the casino management system (**SYCO**), rather than recording each individual deposit as a separate entry.[41] These aggregation errors obscured the number and nature of the deposits[42] which did not give the Crown AML team visibility over what was occurring in the underlying bank accounts and did not allow them to properly monitor the AML risks.

[36] Bergin Report Vol 1 – Section 3.2 paragraph 11

[37] Bergin Inquiry Vol 1 – Section 3.2 paragraph 2

[38] Bergin Inquiry Vol 1 – Section 3.2 paragraph 3

[39] Bergin Inquiry Vol 1 – Section 3.2 paragraph 154

[40] Bergin Inquiry Vol 1 - Section 3.2 paragraph 61-64

[41] Bergin Inquiry Vol 1 - Section 3.2 paragraph 31

[42] Bergin Inquiry Vol 1 - Section 3.2 paragraph 33

(c) These aggregation errors were occurring as late as October 2018 and were still continuing after that time,[43] showing significant deficiencies in the transaction monitoring of the Southbank and Riverbank accounts during that period.[44]

(d) In January 2014, ANZ's internal investigations had identified a series of suspicious transactions in the Riverbank account, being multiple deposits on the same day at different Perth branches of cash amounts of under $10,000 by the same person.[45] Ken Barton (Director of Riverbank) admitted in his Third Statement to the Bergin Inquiry that the steps taken by Crown following ANZ's concerns were "inadequate" and there should have been a thorough review of the Southbank and Riverbank accounts at the time.[46]

(e) The Bergin Report concluded that *"The manner in which Crown has dealt with the allegations in respect of the Southbank and Riverbank accounts demonstrates not only a failure to understand the anti-money laundering landscape and legislative requirements but also a total lack of commitment to turning inwards and rectifying the obvious problems that were identified on 5 and 6 August 2019 in the article..."*[47]

4.3 Crown's investigations into Southbank and Riverbank

4.3.1 The following provides an overview of the various investigations instigated by Crown into transactions in the Southbank and Riverbank accounts following the Media Allegations

Internal reviews

4.3.2 Louise Lane (then Group General Manager of AML) requested the bank statements of the Southbank account on 6 August 2019 and over the next two weeks conducted a manual review of the statements, cross-checking suspicious activity with SYCO entries and checking whether Crown had appropriately submitted SMRs.[48]

4.3.3 On 21 August 2019, Ms Lane advised Joshua Preston (Legal Officer and AML Compliance Officer for Crown Perth) that a more detailed review should occur and she suggested engaging Grant Thornton to investigate the accounts.[49] No such review proceeded at that time.

4.3.4 Claude Marais, General Manager Legal and Compliance reported by memo to Mr Barton (CEO) on 29 September 2020 in respect of an internal investigation undertaken into cash deposits in the accounts of Riverbank (across two bank accounts from July 2013 to December 2019) and Southbank (one bank account from October 2013 to December 2019).

4.3.5 Mr Marais reported that multiple deposits had been aggregated when they were input to SYCO which meant that they were not identified as individual deposits when reviewed by the AML team in accordance with the transaction monitoring program. The memo summarises the outcome of the investigation as identifying 102 instances of aggregation, involving 609 cash deposits and 61 patron accounts, involving funds in excess of $5.2m.[50]

Initialism and Grant Thornton reviews

4.3.6 On 14 October 2020 Crown engaged Grant Thornton to assist with forensic data analysis of the Southbank and Riverbank bank statements. Initialism was also engaged to consider Grant Thornton's analysis of the Southbank and Riverbank accounts for indications of money laundering. These reports were provided to the Bergin Inquiry in mid-November 2020.

[43] Bergin Inquiry Vol 1 - Section 3.2 paragraph 75

[44] Bergin Inquiry Vol 1 - Section 3.2 paragraph 70

[45] Bergin Inquiry Vol 1 - Section 3.2 paragraph 48

[46] Bergin Inquiry Vol 2 - Section 4.3.2 paragraph 63

[47] Bergin Inquiry Vol 2 - Section 4.5 paragraph 31

[48] Bergin Inquiry Vol 1 - Section 3.2 paragraph 97

[49] Bergin Inquiry Vol 1 - Section 3.2 paragraph 100

[50] GTA.001.0001.1012

4.3.7 According to the Initialism analysis, *"cuckoo smurfing exploited legitimate payments relating to gaming activity by Crown's customers, interceding in the payment flow and replacing legitimate funds en-route to Crown."*[51]

4.3.8 The Initialism Report identified numerous transactions in the Southbank and Riverbank accounts which they assessed as indicative of ML:[52]

4.3.9 As a result of the Initialism analysis, the Bergin Inquiry reported:

(a) The use of third-party companies and overseas money remitters to deposit money presented a risk of money laundering due to the identity of the individual making the deposit being obscured and any audit trail being difficult to follow.[53]

(b) From as early as November 2014, Crown gave instructions that deposits were only to be made from personal accounts, however it is clear that these instructions were ignored and not enforced.[54]

4.3.10 In his statement to the Commission dated 25 April 2021, Nick Stokes, Group General Manager AML and AML/CTF Compliance officer stated that as a result of the internal investigations, Crown had submitted SMRs to AUSTRAC as follows:

(a) 51 SMRs in respect of potential structuring in the Riverbank bank accounts;

(b) 8 SMRs in respect of potential structuring in the Southbank bank account; and

(c) 5 SMRs in relation to other potential ML/TF indicative transactions identified through Grant Thornton and Initialism's review of the Riverbank and Southbank bank accounts.

The Deloitte review

4.3.11 The Bergin Report refers to the need for a "*full and wide ranging forensic audit of all [of Crown's] accounts to ensure that the criminal elements which infiltrated Southbank and Riverbank have not infiltrated any other accounts*".[55]

4.3.12 On 22 February 2021 Crown engaged Deloitte to undertake an investigation into transactions by patrons across all bank accounts. In its engagement letter,[56] Deloitte refers to being asked to conduct a review as set out in Crown's current proposed letter to the Independent Liquor and Gaming Authority (New South Wales) (**ILGA**) and describes the purpose of the services to be provided as:

"to assist you in addressing specific suggestions made in the Bergin Report as part of a broader pathway to render Crown Sydney and Crown resort as a "suitable" casino licensee"

4.3.13 The scope addressed by Deloitte is set out in Table 10 in section 4.6.2 of this report. No reports of Deloitte's investigation into indicators of money laundering in Crown's bank accounts have been made available as at the date of this report.

4.4 Crown's response - policy and process changes

4.4.1 The Bergin Report states that on the basis of the Initialism report, Crown acknowledged that from 18 November 2020 it was "*more probable than not*" that money laundering, specifically cuckoo smurfing activity, had occurred in the Southbank and Riverbank accounts.[57]

4.4.2 Crown has implemented a number of policies and rules aimed at preventing and detecting the use of Patron Bank Accounts to facilitate money laundering. These include the following which are addressed in further detail in section 6 of this report:

(a) Elimination of the practice of aggregating deposits in SYCO (refer 6.2).

[51] INI.0002.0001.3272

[52] INI.0002.0001.3272

[53] Bergin Inquiry Vol 1 - Section 3.2 paragraphs 142-143

[54] Bergin Inquiry Vol 1 - Section 3.2 paragraph 146

[55] At p569 para 16

[56] DTT.005.0001.0001

[57] Bergin Inquiry Vol 1 - Section 3.2 paragraph 126

(b) Third Party Transfers and Money Remitters policy issued on 16 November 2020 (refer 6.3).

(c) Bank Statement Monitoring processes (refer 6.4).

(d) Return of Funds policy issued on 4 January 2021 (refer 6.5) including prohibition on cash deposits to Crown accounts.

4.5 Banking and accounting for patrons' monies

4.5.1 Funds deposited by patrons into a Patron Bank Account are accounted for by Crown as follows:

(a) The deposit in the bank account is accounted for as an asset; it is one of the elements of cash at bank disclosed in Crown's balance sheet which also includes funds in other bank accounts held by Crown and used for operation purposes (e.g. to pay payroll, trade creditors and receive rental income etc.).

(b) The receipt of patron monies gives rise to a corresponding liability to the patron which is recorded in the patrons DAB Account and the total of DAB all accounts is described as "Patron Account Liability" and included in current liabilities in Crown's balance sheet, net of any debt owed to Crown by the respective patrons[58].

4.5.2 The total of the DAB accounts is reconciled to Crown's financial accounts on a monthly basis.

4.5.3 Crown currently operates 7 Patron Bank Accounts as shown in Table 7.

Table 7

Patron Bank Accounts at June 2021

Entity	Account name	Bank	Account number	Currency
Crown Perth	Casino CCC	ANZ	[redacted]	AUD
Crown Melbourne	Crown MLB STA	ANZ		AUD
Crown Melbourne	Crown Melbourne	ANZ		SGD
Crown Melbourne	Crown Melbourne	ANZ		GBP
Crown Melbourne	Crown Melbourne	ANZ		HKD
Crown Melbourne	Crown Melbourne	ANZ		USD
Crown Melbourne	Crown Melbourne	ANZ		USD

Source: Crown AML Manual Bank Statement Review Guidelines [CRW.510.039.3515]

4.5.4 The funds in the Patron Bank Accounts are transferred on a daily basis to Crown's main operations account and the accounts are also used for deposits from and payment to Prosegur[59] which handles secure cash movements to and from the Cage. Accordingly, the balance in the bank accounts does not represent the deposits made by or balance owed to patrons. The funds deposited by patrons is not held on trust; it is combined with Crown's own funds.

4.5.5 Crown does not pay interest for the use of patron funds and does not systemically account to patrons for the funds held. Patrons can seek a report of their DAB and SK account balance and transactions from the Cage.

4.5.6 We observe:

(a) The Patron Bank Accounts are not administered in accordance with the custodial or reporting obligations which would apply if such funds were held on trust for the patrons;

(b) Patron funds are accounted for as a current liability of Crown. The funds are available for use by Crown and the interest of the patrons is as unsecured creditors of Crown; patrons are reliant on Crown's continued solvency to recover the monies they have advanced to Crown; and

(c) Crown has no prudential obligations as would be the case if it were a deposit taking institution.

---

[58] [redacted] manager advised that a monthly reconciliation is performed where debt owed by patrons is netted off against DAB/SK Accounts to report the net debt. Copies of certain of these reports were requested under a Notice to Produce, but were not received in tome to be taken into account in this report.

[59] Third party secure transport provider

4.5.7 Whilst it is the case that Crown has long had a practice of accepting funds from patrons and holding them to facilitate patrons' future gaming, the nature of the arrangement lacks the governance typically required when an entity has custody of third party funds.

4.6 DAB Accounts and Safekeeping Accounts

4.6.1 A report provided by Crown[60] shows the liability of Crown as at 15 June 2021 to patrons of Melbourne Casino totalled $47.1 million as summarised in Table 8.[61]

Table 8

DAB and Safekeeping Account balances 15 June 2021 - Melbourne

	DAB	Safekeeping	Total
No of accounts with balances	2,438	89	2,516
Total value	**21,969,415**	**25,148,126**	**47,117,541**
Mean average	9,011	282,563	18,727
Median	156	4,126	174
Largest balance	1,500,000	7,079,079	7,079,089

11 patrons have both a DAB and a Safekeeping account balance

One patron has a HKD Safekeeping account with a balance of HKD3.7 m (approx $630k)

Source: CRW.512.152.0004 (Melb)

4.6.2 Deposited funds are described as either DAB accounts or Safekeeping accounts. [redacted] described and distinguished these two types of accounts as follows:

(a) When a patron opens a DAB account, a Safekeeping account is also available, although not always availed of by patrons.

(b) The DAB account is typically the account which patrons use for day to day transactions.

(c) The Safekeeping account is used in different ways by different patrons; for example some like to "bank" their winnings in it to distinguish them from deposited funds; some like to build a balance to repay debt owed to the casino as and when it is due.

(d) They are both subject to the same rules and controls as each other when it comes to deposits and withdrawals as set out in the Standard Operating Procedures (**SOP**) Cage Operations,[62] including undergoing the applicable customer identification process (**ACIP**).

(e) There is no difference in how the funds may be deposited into Crown's bank accounts, the difference is only in the accounting by Crown.

4.6.3 Crown employees have suggested[63] that some patrons use the DAB/Safekeeping facility in preference to a regular bank and suggest that this may be because:

(a) There are no transaction fees or charges;

(b) The Casino is open 24 hours a day 7 days a week; and

(c) Some patrons distrust banks.

4.6.4 Analysis of the patron DAB and Safekeeping balance report at 15 June 2021[64] shows that:

(a) Notwithstanding [redacted] advice that patrons use the two accounts for different purposes, at 15 June 2021, only 11 patrons had a balance in both the DAB and the Safekeeping accounts:

---

[60] CRW.512.152.0004 KKPatron Deposit Status Report

[61] CRW.512.152.0004 also shows that a further $18m is owed to Perth Casino patrons of which $12.4 million in Safekeeping accounts

[62] CRW.510.013.273 at 4.5 et seq

[63] In a Focus Group

[64] CRW.512.152.0004 Patron Deposit Status Report

(i) 2,427 patrons had only a DAB balance; and

(ii) 78 patrons had only a Safekeeping balance.

We acknowledge this may be because the Casino was then in lockdown and international travel was limited by COVID-19 considerations.

(b) As set out in Table 9 below:

(i) 87% of DAB accounts have balances of less than $10,000 and less than 1% of accounts (3 patrons) hold more than $1 million.

(ii) In the Safekeeping accounts, 65% of the accounts hold less than $10,000 and 7% (6 patrons) hold more than $1 million representing 91% of the total value of the Safekeeping accounts.

Table 9

DAB and Safekeeping Account balances 15 June 2021 - Melbourne

	DAB Accounts				Safekeeping Accounts			
Account balance	**No**	**% No**	**Value $'000**	**% Value**	**No**	**% No**	**Value $'000**	**% Value**
>$5m	-	*0%*	-	*0%*	2	*2%*	12,895	*51%*
$1m to $5m	3	*0%*	3,808	*17%*	4	*4%*	10,159	*40%*
$500k to $1m	4	*0%*	2,832	*13%*	-	*0%*	-	*0%*
$200k to $500k	12	*1%*	3,063	*14%*	4	*4%*	1,117	*4%*
$100k to $200k	21	*1%*	3,121	*14%*	-	*0%*	-	*0%*
$50K to $100k	39	*2%*	2,676	*12%*	8	*9%*	597	*2%*
$10k to $50K	224	*9%*	4,783	*22%*	13	*15%*	259	*1%*
$1k to $10K	400	*17%*	1,437	*7%*	31	*35%*	117	*0%*
<$1k	1,656	*70%*	249	*1%*	27	*30%*	4	*0%*
	2,359		**21,969**		**89**		**25,148**	

Source: CRW.512.152.0004 (Melb)

4.7 Deloitte review

4.7.1 On 22 February 2021 Crown executed a letter of engagement with Deloitte pursuant to which Deloitte was to provide services in 3 phases.[65]

4.7.2 The purpose of the Deloitte engagement as set out in its engagement letter dated 22 February 2021[66] is:

"to assist you [Crown] in addressing specific suggestions made in the Bergin Report as part of a broader pathway to render Crown Sydney and Crown Resort as a "suitable" Casino licensee"

The letter identifies the suggestions of the Bergin report referred to in the purpose statement as:

(a) The conduct of a full and wide ranging forensic audit of Crown resorts and Crown Sydney's bank accounts.[67]

(b) Building strong barriers against criminal infiltration of Crown's bank accounts.[68]

4.7.3 Table 10 is a summary of the work to be undertaken in each phase and the current status of that work.

[65] DTT.005.0001.0001 Note that the original period for the review of transactions was a 3 year period, this was later extended to a 7 year period to February 2021 DTT.002.0001.6480.

[66] DTT.005.0001.0001

[67] Bergin report p569 para 16

[68] Ibid page 569 para 15

Table 10

Deloitte review of Patron Bank Accounts

Phase	Description	Status	Note
1	An assessment of the design effectivness and the operational effectveness of controls pertaining to Patron Bank Accounts in the period from 1 December 2020 to 22 February 2021	Complete	(a)
2(i)	A forensic investigation to identify all bank accounts associated with Crown into which patrons could deposit funds for the period January 2013 to February 2021	Complete	(b)
2(ii)	A forensic analysis of transactions in Patron Bank Accounts identified in Phase 2(i) to identify activity indicative of ML/TF typologies	In progress; est completion by 27 August 2021	(c)
3	An assessment of the design effectiveness and operational effectiveness of a broader set of Crown's controls insofar as they relate to ML/TF typologies and any ML/TF activity identified in Phase 2(i)	Not started; est. completion by 27 August 2021	(c)

Notes

(a) Draft report issued 26 March 2021 [DTT.005.0001.0038]

(b) This work has not been reported upon but Deloitte has provided the Commission with Workpapers prepared to support its Phase 2(ii) work [DTT.010.0004.0032] and [DTT.101.0004.0030]

(c) Deloitte status report dated 7 May 2021 indicated Phase 2 bank account analysis would be completed by 25 June 2021 and additional work investigating patron related data for patrons associated with potential ML/TF activity would be completed by 27 August 2021 [DTT.999.0001.0001]

4.7.4 We note that Deloitte's scope appears limited to a review of the bank account transactions. In our view, it is necessary to consider the transactions in the bank accounts and also how they are reflected, and how the funds subsequently transacted, within the DAB/SK accounts in order to gain a fulsome picture of what has transpired. It is likely that additional information including gaming records and UAR/SMR activity would be necessary to gain a full understanding of the patrons' actions and whether they are indicative of ML.

4.7.5 As at the date of this report, Deloitte had not completed or reported its Phase 2(ii) analysis of transactions in the patron bank accounts. In order to provide the Commission with the benefit of some analysis of Patron account transactions, we have undertaken a limited analysis of the transactions in both the Patron Accounts and the DAB/SK accounts. Our methodology, findings and limitations are set out in section 5.

4.7.6 Deloitte's assessment of each of the new patron account controls is addressed in section 6 of this report.

5 McGrathNicol review of transactions in patron bank and DAB/SK accounts

5.1.1 As indicated in Table 10, Deloitte did not anticipate completing its analysis of transactions in the Patron Bank accounts until 27 August 2021 which is expected to be after the Commission has completed its hearings. In view of this, McGrathNicol was instructed to undertake a review of the transactions through the Patron Bank Accounts in the period 1 July 2019 to 22 February 2021.

5.1.2 The methodology adopted to investigate transactions through the Patron Bank Accounts and our findings are detailed in Appendix B and summarised as follows.

5.2 Methodology

5.2.1 The following primary data sets were procured under notices to produce issued by the Commission:

(a) From Deloitte - the Patron Bank Account transaction data provided to Deloitte by Crown for all Patron Bank Accounts[69] for the period 1 July 2019 to 22 February 2021 (**PBA data**) - received by McGrathNicol on 23 June 2021; and

(b) From Crown - DAB account data comprising:

(i) The balance of all patron DAB Accounts with balances as at 15 June 2021 (**DAB balance data**) – received by McGrathNicol on 18 June 2021; and

(ii) All transactions recorded for patron accounts in the period 1 January 2019 to 15 June 2021 (**DAB transaction data**) - received by McGrathNicol on 18 June 2021.

5.2.2 The following steps were undertaken for further analysis of the PBA data:

(a) Data from relevant Patron accounts were compiled into a single dataset for analysis;

(b) The narrative field was used to extract potential references to the DAB accounts within which the funds were to be directed; Table 11 below details the breakdown of the matched transactions; and

(c) Details of the transaction type (transfer, direct credit, cash etc.) were inferred from the content of the narrative also.

Table 11

Account Name	Account Number	Earliest date	Most recent date	Total transactions
BURSWOOD NOMINEES LTD ATFBURSWOOD PROPERTY TRUST	[redacted]	2019-07-01	2021-02-19	376
Crown Melbourne Limited		2019-07-01	2021-02-22	4,652
Riverbank Investments Pty Ltd		2019-07-03	2019-10-14	30
Southbank Investments Pty Ltd		2019-07-01	2019-11-30	1,679
Southbank Investments Pty Ltd		2019-07-15	2019-11-21	9

Source: McGrathNicol

5.2.3 The following steps were undertaken for further analysis of the DAB transaction data:

(a) The DAB transaction data was provided separately for each property (Melbourne and Perth), for the purposes of this analysis the data from both properties were combined into a single dataset;[70]

[69] As identified by Deloitte through its detailed review of banks accounts

[70] A single instance of two individuals at each location having the same patron ID was noted, we are unable to identify if this was a typographical error or genuine accounts, as such this patron ID was excluded from the analysis

(b) linked patron DAB accounts were combined off either the linked accounts provided by Crown[71] or through linkage by date of birth, surname, and last name; and

(c) full descriptions of the 'Account Type', 'Doc Type, and 'Type' columns were obtained from the glossary provided[72] and added to the dataset.

5.2.4 Further details of the analyses can be found in their respective sections below or in full detail in Appendix B.[73]

5.3 Assumptions and limitations

5.3.1 Our findings are set out below and should be read subject to the following:

(a) When isolating transactions relevant to the analysis within the DAB account data, the type of account involved was derived from the 'Account Type' column in the raw data and account types were aligned to the glossary provided.[72]

(b) When isolating deposits into the DAB and Safekeeping accounts the 'Doc Type' column was used to identify deposits according to the glossary.[72]

(c) When isolating cash transactions only within the DAB and Safekeeping accounts the 'Type' column was used and aligned with the glossary.[72]

(d) McGrathNicol is aware that a single individual can hold more than one DAB account and thus have more than one patron ID associated with them. To group these accounts, we conducted a manual review of instances where unique accounts were held by individuals with the same date of birth, surname, and similar first names. All linked accounts identified had first names which were at least 90% similar.

(e) Tie Baccarat accounts were not considered in the analysis.

5.4 "Parking" of funds

5.4.1 Parking of funds may be indicative of ML activity because it creates a temporal distance between the source and the use of the funds and in this way is a form of layering.

5.4.2 To assess the parking of funds, the balance of the DAB/SK accounts (from the DAB Balance Data) was compared the last recorded transaction (of any kind) on that patrons account (from the DAB Transaction Data). The analysis was restricted to accounts with a balance of $50,000 or more.

5.4.3 Our analysis resulted in the following findings:

(a) 97 accounts were found to have a balance of $50,000 or more at the time the balances were provided (15 June 2021).

(b) 30 patron accounts (comprising 3 SK accounts and 27 DAB accounts) have not had a transaction recorded since 2019 with the highest balance of these accounts being $1,500,000 (patron ID [redacted]056 DAB account).

(c) 46 patron accounts (comprising 35 DAB accounts and 13 SK accounts) have not had a transaction recorded since 2020 with the highest balance of these accounts being $7,079,089 (patron ID [redacted]488):

(i) Five of these accounts have a most recent transaction after 30 June 2020 (one DAB account and four SK accounts).

(ii) The most recent transactions for the remaining 41 accounts occur between 1 Jan 2020 and 30 June 2020.

(d) The remainder of accounts had transactions recorded in 2021 with the highest balance of these accounts being $1,337,169 (patron ID [redacted]755).

---

[71] CRW.512.152.0001

[72] Allens letter relating to NTP-172 dated 18 June 2021

[73] Appendix B provides an index to a digital file which includes details of methodology and the results of the analysis in full detail, including references to the transactions reported in our findings in this report.

5.4.4 Examples of the transactions identified include:

(a) According to the DAB Balance Data patron ID [redacted]056 had a balance of $1,500,000 in their DAB account and a balance of $0 in both their Safekeeping and Tie Baccarat accounts as of 15 June 2021:

(i) The DAB Transaction Data shows two transactions in respect of patron ID [redacted]056, both on 17 July 2019 at the same time (13:10:07).

(ii) One transaction was a telegraphic transfer deposit of $3,000,000 and the other was a Direct (free text) transfer withdrawal of $1,500,000. We did not observe the $3,000,000 deposit in the bank account; we have assumed this occurred prior to 1 July 2019.

(b) The patron account ID [redacted]488 with a balance of $7,079,089 (an SK account) has over 1200 transactions recorded with 70 of these transactions having a value greater than $1,000,000.

5.4.5 The analysis to identify potentially "parked" funds is subject to the following specific caveats or limitations:

(a) This analysis relied on the completeness of the DAB Transaction Data provided to us to calculate the last transaction on the account.

(b) The restrictions imposed due to COVID-19 and the effect this had interstate travel and patron activity within the Casino may be a factor in the interpretation of the data.

5.5 Transactions indicative of structuring in DAB Accounts

5.5.1 Structuring is the breaking down of transaction which would be subject to regulatory reporting into smaller transactions which are below the reporting threshold. It may be indicative of ML and if it is done with the intent to avoid reporting, it is illegal.

5.5.2 For the purpose of this analysis, transactions indicative of structuring was defined as two or more cash deposits in respect of a single patron below $10,000 that, when combined over a set period (24, 48, or 72 hours), totalled to be more than $10,000.

(a) The nature of the transaction (withdrawal or deposit) was derived from the 'Doc Type' column.

(b) The type of transaction (cash or otherwise) was derived from the 'Type' column.

(c) Analysis was completed across all cash deposit transactions on a patrons DAB and Safekeeping accounts.

(d) In instances where multiple accounts were identified (5.3.1(d)) all transactions for the individual were treated as one account.

(e) When calculating the combined transaction value, the relevant period (24, 48, or 72 hours) was calculated retrospectively from the timestamp on the transaction. All transactions that fell within that defined period prior to the transaction were totalled creating a rolling total representing the period of interest and all transactions that fall within it.

(f) The analysis includes all transactions that met the criteria within that period, even if it met the criteria of another period. For example, two $9,000 transactions 10-minutes apart would meet the criteria for and be found in the 24-, 48-, and 72-hour analyses.

5.5.3 Our analysis resulted in the following findings:

(a) When assessing transactions indicative of structuring over a 24-hour period, 481 instances where a combination of transactions < $10,000 summed to over $10,000 within a 24-hour window, involving:

(i) 908 individual transactions;

(ii) 174 patron IDs (after combining linked patron IDs into a single entity);

(iii) $4,506,892 worth of deposits (average deposit value of $4,963); and

(iv) The most recent instance at the Melbourne property was on 12 May 2021 and 19 April 2021 at the Perth property.

(b) When assessing transactions indicative of structuring over a 48-hour period, 833 instances where identified transactions of less than $10,000 over a 48-hour period exceeded $10,000 when combined, involving:

(i) 1,472 individual transactions;

(ii) 240 patron IDs (after combining linked patron IDs into a single entity);

(iii) $6,925,540 worth of deposits (average deposit value of $4,705); and

(iv) The most recent instance at the Melbourne property was on 25 May 2021 and 16 June 2021 at the Perth property.

(c) When assessing transactions indicative of structuring over a 72-hour period, 1,103 instances where identified transactions of less than $10,000 over a 72-hour period exceeded $10,000 when combined, involving:

(i) 1,914 individual transactions;

(ii) 272 patron IDs (after combining linked patron IDs into a single entity);

(iii) $8,734,498 worth of deposits (average deposit value of $4,563); and

(iv) The most recent instance at the Melbourne property was on 25 May 2021 and 16 June 2021 at the Perth property.

(d) Overall, the vast majority of instances involved DAB accounts with less than 1% of the transactions involving SK accounts (22 transactions).

5.5.4 Examples of the transactions identified include:

(a) Figure 2 below shows six cash deposits into the DAB account of patron [redacted]300 recorded for Melbourne on 22-25 February 2021. The total value of the transactions is $29,500 and is made up of transactions of values $2,500, $3,500, $4,500, $5,000, $6,000, and $8,000.

Figure 2

MCN Principle account #	Stop	First Name	Last Name	Account	Type	Date	Time	Amount	Prev 24hr Total	Location	Property
99012300	FXP	[redacted]		Deposit Account (DAB account)	Cash (AUD/HKD)	22/02/2021	14:05:51	2500	2500	FW01	Melbourne
99012300	FXP			Deposit Account (DAB account)	Cash (AUD/HKD)	22/02/2021	22:16:28	3500	6000	FW03	Melbourne
99012300	FXP			Deposit Account (DAB account)	Cash (AUD/HKD)	23/02/2021	13:44:19	4500	10500	FW03	Melbourne
99012300	FXP			Deposit Account (DAB account)	Cash (AUD/HKD)	24/02/2021	20:31:54	6000	6000	FW03	Melbourne
99012300	FXP			Deposit Account (DAB account)	Cash (AUD/HKD)	25/02/2021	0:22:51	5000	11000	FW01	Melbourne
99012300	FXP			Deposit Account (DAB account)	Cash (AUD/HKD)	25/02/2021	22:15:33	8000	13000	FW03	Melbourne

Source: McGrathNicol analysis – refer Appendix B

(b) Figure 3 shows seven cash deposits into the DAB account of patron [redacted]584 recorded for Perth on 16-25 January 2021. The total value of the transactions is $55,000 and is made up of transactions of values $1,000, $4,000, $5,000 (x4), $7,000 (x2), and $8,000 (x2).

Figure 3

MCN Principle account #	Stop	First Name	Last Name	Account	Type	Date	Time	Amount	Prev 24hr Total	Location	Property
12882584	B	[redacted]		Deposit Account (DAB account)	Cash (AUD/HKD)	16/01/2021	20:51:28	5000	5000	FW16	Perth
12882584	B			Deposit Account (DAB account)	Cash (AUD/HKD)	16/01/2021	22:19:35	7000	12000	FW16	Perth
12882584	B			Deposit Account (DAB account)	Cash (AUD/HKD)	17/01/2021	20:47:35	5000	17000	FW15	Perth
12882584	B			Deposit Account (DAB account)	Cash (AUD/HKD)	19/01/2021	21:37:13	8000	8000	FW15	Perth
12882584	B			Deposit Account (DAB account)	Cash (AUD/HKD)	20/01/2021	20:27:34	5000	13000	FW16	Perth
12882584	B			Deposit Account (DAB account)	Cash (AUD/HKD)	22/01/2021	19:34:08	4000	4000	FW15	Perth
12882584	B			Deposit Account (DAB account)	Cash (AUD/HKD)	22/01/2021	19:35:11	1000	5000	FW15	Perth
12882584	B			Deposit Account (DAB account)	Cash (AUD/HKD)	22/01/2021	20:24:50	8000	13000	FW16	Perth
12882584	B			Deposit Account (DAB account)	Cash (AUD/HKD)	25/01/2021	20:43:13	5000	5000	FW15	Perth
12882584	B			Deposit Account (DAB account)	Cash (AUD/HKD)	25/01/2021	22:02:24	7000	12000	FW16	Perth

Source: McGrathNicol analysis – refer Appendix B

5.5.5 The analysis to identify potential structuring in DAB Accounts is subject to the following specific caveats or limitations:

(a) The transactions identified in the analysis are transactions indicative of structuring according to the definition outlined in 5.5.2 however cannot be definitively identified as structuring. Behaviours such as those shown in the examples at 5.5.4 may relate to genuine gaming behaviour; additional information including the gaming records, past and contemporaneous and potentially a statement of funds declaration (if applicable) would add to an understanding of whether this behaviour was indicative of ML activity.

(b) The analysis was limited to cash deposits into a patrons DAB or safekeeping account (or linked accounts as identified in 5.3.1(d)) and did not consider other Casino Value Instruments (**CVI**).

(c) No transactions in the analysis were identified as a currency other than AUD and thus all amounts were treated at face AUD value.

5.6 Transactions involving third party payments

5.6.1 The payment of third-party monies into patron bank accounts results in Crown not knowing with whom or with whose funds it is dealing which offends its KYC obligations and may be indicative of cuckoo smurfing activity. In 2020, Crown policy changes such that Third Party Payments were no longer accepted into DAB/SK accounts.

5.6.2 The testing process undertaken is described as follows:

(a) The analysis was restricted to deposits into Patron accounts.

(b) All sets of numbers were extracted from the narrative field of the PBA and checked against the DAB Account Data we were provided with to check for a direct match to a known patron account.

(c) The narrative field from the bank account data was then checked if it contained a match to the known DAB account surname or first name.

(d) Those instances where no match for the DAB account holders first or surname could be found in the narrative field the transactions were then aligned against the dates when messaging surrounding the policy to not accept acceptance of third-party transfers was disseminated within Crown.[74]

(e) Those instances where no match for the DAB account holder's first or surname could be found in the narrative field the transactions were then manually reviewed and highlighted where the non-match was confirmed, such that it could reasonably be concluded that it was a third party deposit.

5.6.3 Our analysis resulted in the following findings:

(a) Overall, from the PBA data considered for analysis (5,578 transactions) 681 instances were found where a transaction was matched to a known DAB account, but the narrative did not contain a name consistent with that of the DAB account holder. These involved 166 patron accounts with one of those patron accounts ([redacted]488) having over 100 instances.

(b) McGrathNicol understands that an Executive Office Memorandum was issued on the 8 April 2020 prohibiting the acceptance of third-party funds into its accounts.[74] The dataset relating to after this date was reduced to 45 instances after this date. This resulted in 45 instances involving 20 patron accounts of which:

(i) 18 instances identified has having no name at all or a highly similar name.

- We have accepted the "no name" transactions as not being third party transfers on the assumption that the patron has presented at the Cage and been able to verify the deposit from their own account through production of bank statements. We do not have the information to verify this assumption and we note that neither "no name" nor "similar name" deposits would comply with Crown policy after 4 January 2021 under the Return of Funds policy.

(ii) 27 instances where the patron name and the narration did not match (including 11 instances for one patron - ID [redacted]755).

(c) A further iteration of the prohibition on third party transfers was issued on 21 October 2020,[74] therefore the dataset was further reduced to assess transactions after this date. We found:

[74] CRW.512.023.0100

(i) 18 transactions after 21 October 2020 of which only one transaction was identified as a "no match" (a potential third party payment) the remainder either had no name or a very similar name e.g. (Salamon versus Soloman).

(ii) The "no match" instance had a very complex string of letters and numbers in the narrative field and thus it cannot be certain that this isn't matched to another account, further data such as internal data linking the bank transaction specifically to the DAB account it was credited against would be required to confirm this.

(d) McGrathNicol understands that on 16 November 2020 a policy was issued entitled "Third Party Transfers and Money Remitters Policy".[74] The transactions that occurred after this policy was introduced is identical to the set of transactions which occurred after 21 October 2020 and the analysis set out at (c) applies.

5.6.4 The analysis to identify potential third-party payments is subject to the following specific caveats or limitations:

(a) 9,717 transactions from the PBA data were identified as being relevant to the analysis, of those, the narratives for 5,578 transactions matched to a known DAB account number (in the DAB transaction data) leaving 4,139 transactions that could not be matched to a DAB account number and this could not be considered in this analysis.

(b) Due to the limited timeframe available, our analysis treated as a match (i.e. not a third-party transfer) deposits where the PBA narrative:

(i) included a sequence of numbers within the narrative on the bank data which matched an account ID of a known patron account; and

(ii) contained an exact match the individual's surname; or

(iii) contained an exact match to the patron's first name.

(c) The 4,139 transactions unable to be matched to a known patron account ID had either:

(i) Numbers/digits present in the narrative that did not correspond to a known DAB account ID; or

(ii) Additional digits/numbers (such as dates etc.) being added to the patron account number; or

(iii) IDs with apparent missing digits.

(d) The final destination of the funds was outside the scope of this analysis, the funds may have been credited to the DAB account identified or returned to the sender.

5.7 Transactions indicative of structuring in Patron (Bank) Accounts

5.7.1 Structuring is the breaking down of transaction which would be subject to regulatory reporting into smaller transactions which are below the reporting threshold. It may be indicative of ML and if it is done with the intent to avoid reporting, it is illegal.

5.7.2 Transactions identified as cash (based on the narratives available in the PBA) and below the value of $10,000 were used for the Patron bank account structuring analysis.

5.7.3 Only transactions where a corresponding DAB account patron ID could be identified were included in the analysis. See 5.6.4 above for further details. This resulted in 17 cash transactions (two < $10,000) unable to be considered in this analysis.

5.7.4 Our analysis resulted in the following findings:

(a) The dataset for cash transactions which matched a DAB patron account comprised 53 transactions.

(b) Of these 53 transactions, two were below $10,000 and were in respect of different patron accounts.

(c) Therefore, based on the criteria outlined in 5.5.2 there were no transactions identified indicative of structuring.

(d) This analysis was restricted to transactions that could be identified as cash and did not look at indications of structuring using a combination of cash and bank transactions. This extended definition of structuring may identify a corresponding bank transfer with the above cash transactions that meet the criteria.

5.7.5 The analysis to identify potential structuring in Patron Accounts is subject to the following specific caveats or limitations

(a) This analysis relied upon the identification of bank accounts by Deloitte outlined in 5.2.1(a).

(b) The limited timeframe prevented a deep reconciliation with those narratives where a clear patron account could not be extracted. As this represented around 30% of the total transactions, a deep reconciliation would likely reveal many more transactions for consideration.

(c) Cash transactions were identified by the word "cash" being present in the narrative. McGrathNicol understands that in some cases the word cash is not mentioned but instead just the branch name. A deeper manual review of the narratives to identify these instances would likely increase the number of transactions to be considered.

5.8 Other Observations

5.8.1 In the course of our analysis we observed that the DAB account of Patron ID [redacted]944 exhibited a repeated pattern of unusual activity involving the use of the ticket-in-ticket-out (**TITO**) CVI.

5.8.2 The behaviour involved many TITO deposits combined with a single large withdrawal (either as a TITO or another CVI). Typically, the TITO deposits were under $10,000 while the single large withdrawal closely reflected the value of the combined deposits. Furthermore, the timestamp associated with all these transactions were either identical or differing only a single minute suggesting these are being processed at the same time.

5.8.3 The screenshot depicted below (Figure 4) shows 14 transactions over a two-minute period comprising 13 deposits and a single withdrawal. The 13 deposits (all under $10,000) total to $106,939 and the withdrawal is for $115,000. Such behaviour is seen on a number of occasions in this account.

Figure 4. Screenshot of example of unusual behaviour involving TITO transactions on patron account [redacted]944.

Location	Property	Account Type	Doc Type	Type	Document Amount	Transaction Datetime
FW01	Melbourne	Deposit Account (DAB account)	Cash Deposit	TITO Ticket (Ticket in Ticket out - Gaming Machines)	9500	3/02/2019 8:48
FW01	Melbourne	Deposit Account (DAB account)	Cash Deposit	TITO Ticket (Ticket in Ticket out - Gaming Machines)	7899	3/02/2019 8:48
FW01	Melbourne	Deposit Account (DAB account)	Cash Deposit	TITO Ticket (Ticket in Ticket out - Gaming Machines)	4464	3/02/2019 8:48
FW01	Melbourne	Deposit Account (DAB account)	Cash Deposit	TITO Ticket (Ticket in Ticket out - Gaming Machines)	4000	3/02/2019 8:48
FW01	Melbourne	Deposit Account (DAB account)	Cash Deposit	TITO Ticket (Ticket in Ticket out - Gaming Machines)	4000	3/02/2019 8:48
FW01	Melbourne	Deposit Account (DAB account)	Cash Deposit	TITO Ticket (Ticket in Ticket out - Gaming Machines)	9630	3/02/2019 8:48
FW01	Melbourne	Deposit Account (DAB account)	Cash Deposit	TITO Ticket (Ticket in Ticket out - Gaming Machines)	9862	3/02/2019 8:48
FW01	Melbourne	Deposit Account (DAB account)	Cash Deposit	TITO Ticket (Ticket in Ticket out - Gaming Machines)	9596	3/02/2019 8:48
FW01	Melbourne	Deposit Account (DAB account)	Cash Deposit	TITO Ticket (Ticket in Ticket out - Gaming Machines)	9988	3/02/2019 8:48
FW01	Melbourne	Deposit Account (DAB account)	Cash Deposit	TITO Ticket (Ticket in Ticket out - Gaming Machines)	9500	3/02/2019 8:48
FW01	Melbourne	Deposit Account (DAB account)	Cash Deposit	TITO Ticket (Ticket in Ticket out - Gaming Machines)	9500	3/02/2019 8:48
FW01	Melbourne	Deposit Account (DAB account)	Cash Deposit	TITO Ticket (Ticket in Ticket out - Gaming Machines)	9500	3/02/2019 8:48
FW01	Melbourne	Deposit Account (DAB account)	Cash Deposit Withdrawal	Chip Purchase Voucher	115000	3/02/2019 8:49
FW01	Melbourne	Deposit Account (DAB account)	Cash Deposit	TITO Ticket (Ticket in Ticket out - Gaming Machines)	9500	3/02/2019 8:49

Source: McGrathNicol analysis – see Appendix B

5.8.4 Another example can be seen in Figure 5 where six TITO deposits total $58,194 and a single TITO withdrawal is for $60,000 all processed at the same time.

Figure 5. Second screenshot of example of unusual behaviour involving TITO transactions on patron account 99005944.

Location	Property	Account Type	Doc Type	Type	Document Amount	Transaction Datetime
FW01	Melbourne	Deposit Account (DAB account)	Cash Deposit Withdrawal	TITO Ticket (Ticket in Ticket out - Gaming Machines)	60000	18/04/2019 11:18
FW01	Melbourne	Deposit Account (DAB account)	Cash Deposit	TITO Ticket (Ticket in Ticket out - Gaming Machines)	9500	18/04/2019 11:18
FW01	Melbourne	Deposit Account (DAB account)	Cash Deposit	TITO Ticket (Ticket in Ticket out - Gaming Machines)	9500	18/04/2019 11:18
FW01	Melbourne	Deposit Account (DAB account)	Cash Deposit	TITO Ticket (Ticket in Ticket out - Gaming Machines)	9500	18/04/2019 11:18
FW01	Melbourne	Deposit Account (DAB account)	Cash Deposit	TITO Ticket (Ticket in Ticket out - Gaming Machines)	9992	18/04/2019 11:18
FW01	Melbourne	Deposit Account (DAB account)	Cash Deposit	TITO Ticket (Ticket in Ticket out - Gaming Machines)	9814	18/04/2019 11:18
FW01	Melbourne	Deposit Account (DAB account)	Cash Deposit	TITO Ticket (Ticket in Ticket out - Gaming Machines)	9888	18/04/2019 11:18

Source: McGrathNicol analysis – see Appendix B

5.8.5 We requested assistance from Crown to understand these transactions on 2 July 2021 but were unable to get a response before finalising this report.

6 AML (patron account) controls

6.1 New AML (patron account) controls

6.1.1 In the last 18 months Crown has introduced a number of policies, rules, practices and guidelines which include controls aimed at mitigating the risk of Patron Bank Accounts being used to facilitate money laundering and/or enabling detection and reporting of such activity (**New AML Regime**).

6.1.2 In February 2021, Deloitte was engaged by Crown to undertake an assessment of the design and operational effectiveness of Patron Bank Accounts controls which were in place from December 2020 onwards. Deloitte issued a draft report of its findings on 26 March 2021.[75]

6.1.3 A summary of the controls relating to patron accounts within the New AML Regime is set out in Table 12. Each control is then further considered together with our observations, commentary on the status of implementation of the controls and, as applicable, the findings reported by Deloitte in relation to Phase 1 of its engagement (as described in section 4.7).

Table 12 Summary of New AML Regime controls relevant to risks of ML in Patron Accounts

Control	Risk targeted	Policy/Rule	Issued	Control(s) / Processes	Refer section
Eliminate aggregation of deposits	Non-detection of structuring	Email instruction (Perth Casino[76])	24 Sept 20	Item 5.1.12 of the SOP Cage procedures[77] states that multiple bank transfers for the same person must never be aggregated into one TT Acknowledgement, by which Crown acknowledges receipt of funds from the patron and records in it their DAB account in SYCO.	6.2
		Email instruction (Melbourne Casino[78])	12 Nov 20		
Refuse third party payments	Transacting with unknown parties Smurfing Cuckoo smurfing	Executive Office Memorandum: Prohibition on Third-Party payments[79]	8 April 20	Crown will no longer make or receive third party payments. The change applies to local, domestic and international customers. Should a customer request a third-party transfer in or out, prior written approval of the COO and Group GM AML is required.	6.3
		Executive Office Memorandum (**EOM**) Prohibition on Third Party Transfers[80]	21 Oct 20	Elaboration on the 8 April 2020 memo reiterating the policy and providing answers to frequently asked questions.	
		Third Party Transfers and Money Remitters Policy[81]	16 Nov 20	Prohibits transfers from third parties including money remitters into or out of Patron Bank Accounts (unless with prior written approval of the property COO and AML/CTF Compliance Officer).	

[75] DTT.005.0001.003

[76] CRW.512.025.0970

[77] SOP Cage Operations (12 Oct 2020) CRW.510.013.273

[78] CRW.512.025.0972 issued as Melbourne Casino re-opened after COVID lockdown according to the Statement of John Salomone dated 21 April 2021

[79] CRW.512.027.1026

[80] CRW.520.003.9552

[81] CRL.742.001.0101

Monitor all transactions	Failure to detect ML activity	Bank statement monitoring rule[82]	16 Nov 20	Requires weekly manual review of all transactions in Patron Bank Accounts to identify: [redacted]	6.4
		AML Manual Bank Statement Review Guidelines[83]	11 Mar 21	Provides guidance for the Financial Crime team as to how to undertake the weekly line by line review of the 7 patron bank accounts (as listed in Table 7) to identify transactions which may transgress the Return of Funds policy or otherwise exhibit characteristics of an ML/TF typology. A UAR is to be created for any transaction which cannot be dispositioned as "no action required" or "already actioned" (e.g. transaction reversed or funds returned).	
Return funds received contrary to policy	Illicit funds placed with Crown Structuring Cuckoo smurfing	Return of Funds Policy	4 Jan 21	From 1 January 2021 Crown will return all payments made to Crown which are not in accordance with the Third Party Transfers and Money Remitters Policy and the Bank Transfer Notification[84] including: ▪ Cash deposits ▪ Third party deposits ▪ Deposits lacking requisite detail Deposits with misleading detail [redacted]	6.5

6.2 Prohibition on aggregation of deposits

6.2.1 The Bergin Inquiry reported that the aggregation of deposits to the Riverbank and Southbank accounts enabled transactions indicative of ML to go undetected.[85] This is consistent with the results of the internal investigation led by Mr Marais (refer 4.3.4).

6.2.2 Such a scenario would play out as follows:

[82] CRL.742.001.0009

[83] CRW.510.039.3515

[84] The Bank Transfer Notification was circulated to patrons within Crown's Platinum and Black membership levels in December 2020 and sets out the manner in which transfers of funds to Crown bank accounts must be made [CRW.512.025.1110]

[85] Bergin Inquiry – Section 3.2 para.116

(a) Cash deposits each of less than $10,000 are made on multiple occasions to the Crown bank account and referenced to a specific patron. These deposits may be made by one person at multiple bank branches or multiple people at one or more bank branches, thereby avoiding threshold transaction reporting by the bank.

(b) The patron presents at the casino Cage with receipts substantiating the deposits and the Cage aggregates the deposits and records them as a single transaction in SYCO which is the primary data source for Crown's AML scrutiny.

(c) As a consequence, SYCO will record the aggregate deposit which exceeds $10,000 but it is:

(i) not recognised as a product of potential structuring because the fact that it comprised multiple deposits is not recorded in SYCO; and

(ii) it may not be recognised as a reportable threshold transaction because the deposits may not be readily recognisable as having been cash transactions.

6.2.3 The control failure is the recording of multiple transactions as a single transaction by the Cage staff. Such a failure is indicative of a lack of ML risk awareness, a lack of AML training and/or inadequate review of the effectiveness of controls.

6.2.4 Following the identification that deposits had been so aggregated, Crown issued instructions on 24 September 2020 to Perth Cage staff and on 12 November 2020 to Melbourne Cage staff[86] requiring them to prepare a separate Transfer Acknowledgement (**TA**) for each individual deposit (i.e. prohibiting the aggregation of multiple telegraphic transfers into a single TA).

6.3 Third party payments not accepted

6.3.1 Acceptance of third party payments into patron accounts provides an avenue for money laundering through smurfing or cuckoo smurfing and results in Crown simply not knowing from whom funds are received which may subvert its KYC obligations in relation to designated services under the AML/CTF Act and Rules.

6.3.2 Removing the acceptance of funds into the patron account from any party other than the patron themselves, eliminates the use of the account for cuckoo smurfing activity and allows Crown to have confidence as to whom it is transacting with, subject to implementation of effective KYC policies and procedures.

6.3.3 Crown issued an EOM on 8 April 2020 prohibiting the acceptance of third-party funds into its accounts and the prohibition was reinforced with the issue of a further EOM on 21 October 2020 which included responses to frequently asked questions.

6.3.4 On 16 November 2020 a policy was issued entitled "Third Party Transfers and Money Remitters Policy".[87] As with the earlier advices, the Third Party Transfers and Money Remitters Policy allows for third party or money remitter deposits with certain senior management approval subject to a specific process being followed which requires:

(a) the preparation of a request by a team member to the AML team to make a recommendation and the information to accompany the request;

(b) the preparation of a recommendation and the evidence to be procured and reviewed by the AML team to enable the AML/CTF Compliance Officer to determine whether to approve the recommendation; and

(c) if the recommendation is approved by the AML/CTF Compliance Officer, a requirement that the property COO approve the transfer before any deposit is accepted.

6.3.5 We have been provided with a copy of the advice sent to patrons in December 2020 which incorporates an advice that funds deposited by third parties will not be accepted and will be returned to the bank account from which they came.[88] We note:

[86] Being the date the Melbourne Casino re-opened after COVID shut down

[87] CRL.742.001.0101

[88] CRW.512.040.0003

(a) The example of the advice to patrons provided to us indicates the advice was sent by email and time stamped 3:03pm on 24 December 2020 - Christmas Eve.

(b) The advice to patrons was issued well after the prohibition on third party deposit was first introduced on 8 April 2020.

6.3.6 Deloitte considered the design and operation effectiveness of the Third Party Transfers and Money Remitters Policy in Phase 1 of its engagement.

6.3.7 Deloitte identified the following limitations to the design effectiveness of this control:[89]

(a) Due to the truncation of information available on the bank account statements, Cage staff are reliant on examination of receipts or bank statements provided by the patron to validate that transfers have come from their own personal bank account. There is residual risk that forged documents may be presented to the Cage. McGrathNicol concurs with this observation.

(b) Non-acceptance of deposits from money remitters relies on the Cage staff knowing or recognising the remitters from the information on the bank statements. Whilst Deloitte suggests further processes to ascertain if the deposit is from a remitter, McGrathNicol is of the view that if the patron is unable to evidence that the deposit is from his/her personal account and the deposit is therefore returned, it is not necessary for the effectiveness of the control to identify from whom the deposit came.

6.3.8 Deloitte tested the operational effectiveness of the Patron Bank Account controls by reviewing all 1,143 transactions in the ANZ account XXXX2834 for the period 1 December 2020 to 21 February 2021 to identify transactions which did not comply with Crown policies.

6.3.9 In respect of the policy to not accept third party deposits, Deloitte initially identified 142 deposits which appeared to be from third parties or lacked the patron name or account number. Of these, funds had been returned in 47 instances, leaving 95 cases for further review. On review of the associated TA packs, 82 cases were resolved leaving 13 unresolved.

6.3.10 The 13 unresolved cases were referred to Crown staff for review and through discussion and walk-throughs by Deloitte with Crown staff, Deloitte obtained explanation and additional documentation which satisfied Deloitte that the patron's full name and ID were provided at the time of the deposit for 11 cases and Deloitte concluded those to be compliant with the policy.

6.3.11 Two cases were found to be unresolved:

(a) A case where the patrons last name was missing and the transaction was accepted on the basis of a previous transaction TA which corroborated the patron's bank account details; and

(b) A case where the patron's bank account is understood by Crown to be held under an alias whilst the patron account is in the patron's real name.

6.3.12 Deloitte assessed these unresolved matters as "deficiencies" rather than "exceptions" on the basis that ultimately Crown, notwithstanding the reasons were not documented in the Transfer Acknowledgement[90] Pack[91] (**TA**), had a rationale for accepting the funds such that the substance of the policy was not offended, albeit the record of the transactions were deficient.

6.3.13 The analysis of bank and DAB/SK account data undertaken by McGrathNicol and described in section 5.6 found one potential instance of third party funds beings deposited to a DAB/SK account after 21 October 2020 and none subsequent to 4 January 2021. We do not have sufficient information to reconcile our finding to Deloitte's.

6.3.14 In his statement dated 25 April 2021,[92] Mr Stokes noted a transaction which had been processed by Cage and Count in breach of the third-party transfer policy on 6 April 2021 as follows:

(a) The Cage processed a payment from a Crown customer to his wife which represented the husband's program settlement funds.

---

[89] DTT.005.0001.0038 at 5.1.2

[90] Being the process through which banked funds are recognized in the patrons DAB account

[91] The pack of documents retained to support acceptance of fund to a DAB account including patron receipt or bank statement

[92] CRW.998.001.0084 - Statement of Nick Stokes 25 April 2021 – para 36-38

(b) Crown staff had used TT information from a previous payment within SYCO which presented them with the wife's details. Cage staff incorrectly assumed their account was a joint account.

(c) As a result, the Cage has introduced a further control on 22 April 2021 that no outgoing transfer is to be processed by VIP banking until Cage and Count Finance Integrity Manager has reviewed.

6.3.15 This example (concerning a payment rather than a deposit) was identified through subsequent review and assurance processes by Crown. This indicates vigilance on Crown's part and a preparedness to continually improve, but equally it highlights that policy is being developed in a reactive manner and in the absence of a rigorous risk assessment process.

6.3.16 We make the following findings and observations, including on the basis of Deloitte's review:

(a) None of the three policy statements (the EOMs of 8 April 2020 and 21 October 2020 and the Third Party Transfers and Money Remitters policy of 16 November 2020) indicates what is to occur if a third party in fact deposits funds in a Crown account. The policy of returning funds appears to have first been communicated in the Bank Transfer Notification (24 December 2020) followed by the Return of Funds Policy issued on 4 January 2021 (refer section 6.5).

(b) Deloitte's review shows that Patrons have not uniformly complied with the changed policy with respect to deposits and in part this may be because the advice although, sent with the email heading "An Important Crown Melbourne Update" was sent on 24 December 2020.

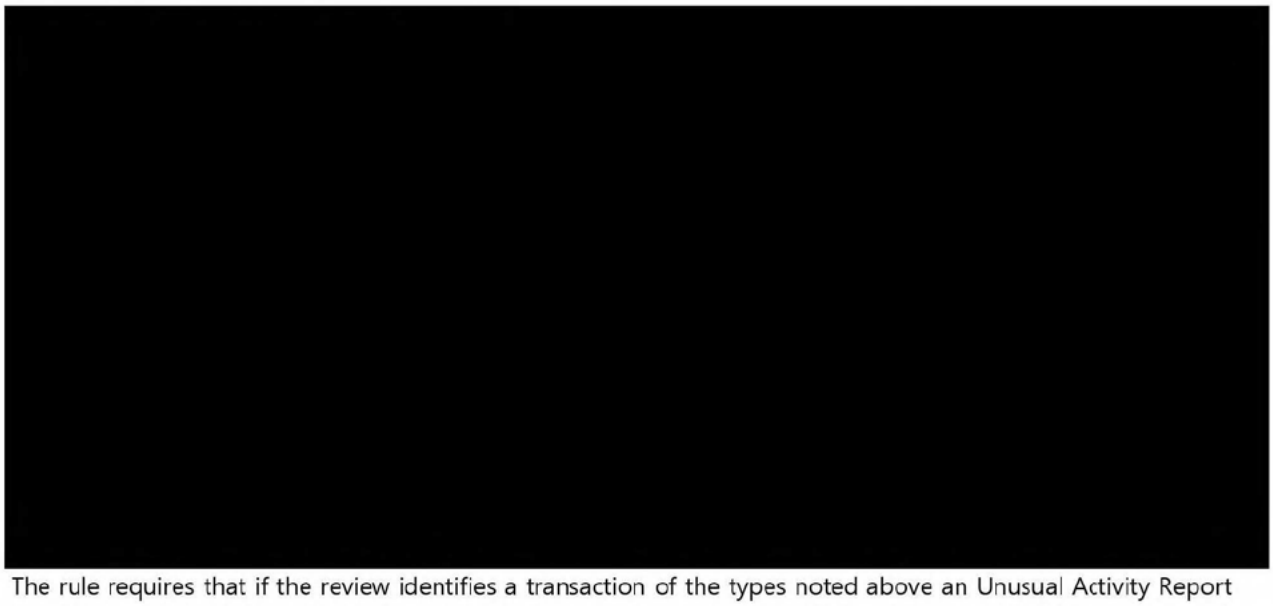
(c) We observe that the process required by Deloitte to work through the paperwork, liaise with staff and undertake walkthroughs in order to assess whether the policy had been operationally effective suggests that compliance is unsustainably difficult to ascertain.

(d) No exceptions (where the funds were accepted contrary to policy) were identified and deficiencies were identified in 2 of the 1,443 transactions reviewed. Deloitte did not report on the value of the deficient transactions nor when the exceptions arose within the review period.

(e) Overall, the new policy of prohibition of Third Party Transfers appears to have been effective. We concur with Deloitte's recommendation[93] that the procedures for documentation within the TA and guidance which will enhance the consistency of documentation and decisions be further developed.

6.4 Monitoring of bank statements

6.4.1 The bank statement monitoring manual rule V1.0 was issued on 16 November 2020 pursuant to Rule 6.2.3 of the Crown Joint AML/CTF Policies and Procedures.

6.4.2 

6.4.3 The rule requires that if the review identifies a transaction of the types noted above an Unusual Activity Report (**UAR**) is to be produced with a copy of the relevant bank statement which involves the AML Team's

[93] Number 14 p40 of DTT.005.0001.0038

consideration of whether the customers risk rating should be raised and whether the customer should be referred to the POI Committee or senior management to approve a continuing business relationship with the customer.

6.4.4 The review of the bank account statements responds to issue identified through the Bergin Inquiry that Crown was not routinely reviewing its banks accounts for AML purposes, only the data held in SYCO was subject to routine review.

6.4.5 [redacted]

6.4.6 Deloitte reviewed the performance of the manual review process of the banks statements for the Crown Melbourne Patron Australian Dollar bank account across 2 weeks. These statements included 183 transactions of which 167, Deloitte considered, as had Crown, did not meet the criteria to trigger a UAR.

6.4.7 Deloitte observed process deficiencies with respect to the remaining 16 transactions including:

(a) Missing patron numbers or reward card numbers without annotation as to the AML Team review and disposition.

(b) Transactions indicative of cash were not annotated but found through discussion with Crown personnel to have been the result of Cage staff banking cheques (not cash).

(c) Transactions annotated by AML Team as having been returned to patrons.

6.4.8 As with the Third Party Payments policy, it appears that in several cases Deloitte had to undertake a walkthrough of the process with Crown personnel in order to ascertain what had been reviewed and the outcome of that review. On this basis, we concur with Deloitte's recommendation the processes need to be further developed to improve consistency and enable efficient review of the effectiveness of the manual rule process.

6.5 Return of Funds

6.5.1 The Return of Funds Policy was issued on 4 January 2021 and provides that from 1 January 2021:

(a) Crown will not knowingly accept funds form a third party;

(b) Crown will only accept payments that are transferred into its bank accounts from the personal bank account of a patron;

[redacted]

[94] The Bank Transfer Notification was circulated to patrons within Crown's Platinum and Black membership levels in December 2020 and sets out the manner in which transfers of funds to Crown bank accounts must be made [CRW.512.025.1110]

(d) Return of cash deposits will be made by the Cage to the patron in cash, no gaming cheques or telegraphic transfers, with a receipt stating it is a *"return of an unauthorised cash deposit"* and a UAR will be raised.

[redacted]

6.5.2 The Return of Funds policy reiterates the Third Party Transfers and Money Remitters Policy and its predecessor EOMs, but adds the prohibition of cash deposits to Crown accounts.

6.5.3 Unlike the earlier policies, the Return of Funds Policy specifies the actions to be taken if patrons fail to observe the policy. In every case where the policy is transgressed, the funds will be returned to where they came from and for cash deposits a penalty for non-observance will be imposed.

6.5.4 Platinum and Black members were advised of the requirements for payments which would not attract the Return of Funds Policy by email in December 2020 (the Bank Transfer Notification[95]) and the Policy states it is effective from 1 January 2021 although it is dated 4 January 2021.

6.5.5 Deloitte reviewed 25 of 69 transactions in the period 1 December 2020 to 22 February 2021 where funds had been returned as recorded in the return of Funds log to test whether the funds had been returned in accordance with the Return of Funds policy.[96] These transactions included transactions which transgressed the Third Party Transfers and Money Remitters policy.

6.5.6 Deloitte found that for all 25 transactions, the funds had been returned in accordance with policy but noted that the tracing of returned funds depended on matching amounts and dates of debit and credit. They recommended the introduction of a unique identifier for returned funds so the return could be readily identified and connected to the patron.

6.5.7 Our review of the minutes of the Person of Interest Committee from November 2020 to February 2021 indicated 2 persons were banned pursuant to the Return of Funds policy (Third Party Payments).

6.6 Findings

6.6.1 We have reviewed Deloitte's methodology and analysis and concur with Deloitte's conclusions in regard to the design effectiveness of the controls within the new AML regime as they relate to patron accounts.

6.6.2 The controls, if implemented, are likely to be effective in deterring cash structuring and cuckoo smurfing activity because:

[redacted]

6.6.3 However, our interviews and focus group discussions together with the results of Deloitte's operational effectiveness review leads us to conclude that the implementation of the policies is immature, materially manual in its processes and there is reason to question their sustainability as trade increases as the COVID-19 impact fades.

---

[95] CRW.512.040.0001

[96] This was in addition to 6 instances of returns of funds identified through the review of the manual bank statement review control

6.6.4 This finding is consistent with Mr Blackburn's assessment of the AML systems overall that they are generally foundational and have some way to go to be consistent and repeatable at higher activity levels. This will involve:

(a) Development of automated systems (refer 7 for consideration of the Sentinel transaction monitoring system which is anticipated to displace the manual review of bank statements);

(b) Documentation of processes to support consistency and assessment of effectiveness of controls; and

(c) Additional resource and ongoing training to ensure controls and implemented consistently and refined to accommodate emerging issues.

7 Transaction Monitoring Program - Sentinel

7.1 Transaction monitoring within the AML/CTF Program

7.1.1 The purpose and scope of the Transaction Monitoring Program is set out in Section 6 of the Joint AML/CTF Policy and Procedures and section 12.3 of Part A of the Crown Joint AML/CTF Program

7.1.2 The purpose of transaction monitoring is to identify, having regard to ML/TF risk, any transaction which appears suspicious within the terms of the AML/CTF Act. Customer activity which is inconsistent with the entity's knowledge of the customer, may be grounds for suspicion.

7.1.3 An entities transaction monitoring program is to be risk-based and take into account the size and complexity of the entity. Crown's Part A transaction monitoring program comprises a suite of systems and controls which includes:

(a) Automated transaction monitoring using Sentinel;

(b) Manual transaction monitoring;

(c) Unusual activity reporting and escalation processes designed to capture potentially suspicious activity identified by employees with customer interaction; and

(d) Manual or exception reporting.

7.1.4 In accordance with the scope of our review we report on our investigations into the Sentinel program.

7.2 Overview of the Sentinel Program

7.2.1 The Sentinel program forms part of Crown's transaction monitoring system and is the internal designated name for the dashboard within which alerts that respond to AML/CTF data analytics rules relevant to the automated monitoring of transactions for relevant ML/TF typologies can be accessed and appropriate action taken by Crown's AML team (**Sentinel**).

7.2.2 Sentinel's underlying architecture is a centralised platform within which relevant alerts are generated from the multiple casino systems. Sentinel was designed with the capability to be continuously updated and refined with rules to match current and emerging ML/TF typologies and risks as they are described by the relevant peak bodies (such as AUSTRAC) (**Sentinel Rules**).

7.2.3 Sentinel was conceptualised in May 2018 with the objective to replace manual transaction monitoring with a contemporary systematic approach and to reduce the large amount of repetitive manual tasks staff were undertaking at the time. McGrathNicol is also advised that the Sentinel program commenced in a basic format by initially performing simple checks on the reports (such as TTRs and SMRs) being sent to AUSTRAC to confirm the information contained in the reports was valid.[97]

7.2.4 Splunk Cloud, a commercial third-party analytics data engine is the data repository for relevant log file data assimilated from Crown's relevant internal ecosystem namely SYCO, DACOM and LUI/CC2 which underpins Sentinel.[98] Log files documenting changes made within these systems are transmitted to the Splunk Cloud platform and analysed in real-time at which time the data is subjected to analysis by the Sentinel Rules.

7.2.5 This approach provides a holistic assessment of the relevant ML/CTF typologies and, importantly, assigns a level of risk to the activity commensurate with the risk associated with the individual customer term rules-based assessment (**RBA**).

7.2.6 The implementation of a project such as Sentinel requires a multidisciplinary team to develop the AML/CTF business rules, collate data and log files, deliver the analytical implementation and overall IT infrastructure development. The following people are members of the 'Centralised Platforms Group' which oversees the Sentinel program:

(a) [redacted] oversees all aspects of Sentinel development and is involved in the platform functionality, rule programming, and platform upkeep.

[97] For example, checking that an address was not listed as a PO Box when a street address was present in the system

[98] Refer to section 7.4 for further explanation regarding data sources

(b) [redacted]

(c) [redacted] support [redacted] in the technical implementation of the project.

(d) [redacted] is responsible for the assessment and development of the AML/CTF business rules and their alignment with the Sentinel Rules, understanding what users require and the investigations team needs.

(e) [redacted] is part of the project management office and is responsible for passing business requirements to the development team and assisting in getting development into production, (the Sentinel Team).

7.2.7 McGrathNicol held a group discussion session with the Sentinel program leaders with the objective of gathering information to assist develop our understanding of the following elements of the Sentinel Program:

(a) The program design;

(b) Data sources;

(c) The development of the Sentinel Rules applied to the data sources; and

(d) The current and planned future state.

7.3 Design of Sentinel

[redacted]

[99] CRW.510.047.1151 - AML Sentinel Source Data List

[redacted]

7.4 Data sources

[redacted]

[100] CRW.512.072.0128 - Initialism Crown Resorts Transaction Monitoring Report

[101] DTT.005.0001.0040

7.5 The Sentinel Rules

7.5.1 The Sentinel Rules are based on typologies identified by authoritative sources such as the Financial Action Task Force, AUSTRAC, Canada's FIU-FINTRAC, the UK Gambling Commission and the American Gaming Association combined with internal subject matter experts and risk assessments.

7.5.2 Crown has identified 51 separate ML/TF typologies from these sources that are relevant to the business. These typologies and Sentinel Rules aimed at capturing them have been investigated by Initialism and key details are reproduced here in Appendix D.

7.5.3 The Sentinel team has advised McGrathNicol that, the implementation priority of the automated rules within Splunk is designed to implement Sentinel Rules targeting the most likely typologies first.

7.5.4 Initialism's report indicates they undertook a review of the typologies identified and the degree to which the proposed automatic transaction monitoring Sentinel Rules would target the relevant typologies. The report states "*...The foundational automated transaction monitoring rules recently implemented by Crown appear to provide coverage of the types of ML/TF Risk Crown may be subject to, the requirements of Chapter 15 of the AML/CTF Rules and the events Crown states it considers in section 6.1.5 of its Joint AML Policy and Procedures.*"

7.5.5 Some of the typologies require analysis to assess financial and gambling activity over a period such as "unusual patterns of physical cash deposits or withdrawals, which are large when aggregated over a period of time."

7.5.6 The specific parameters for these Sentinel Rules are initially developed internally through subject matter expertise. [redacted] informed McGrathNicol that an arbitrary threshold is set in the beginning and the parameters are tuned until "they make sense" and that these parameters will be tuned according to future analysis once sufficient data has been gathered.

7.5.7 McGrathNicol understands that the Sentinel Rules are triggered by location and then by patron. Meaning an individual's behaviour is considered in a location specific manner. This approach may not take into account activity undertaken by patrons at more than the one property.

7.6 Current and planned future state of the Sentinel Program

7.6.1 According to the April 2021 Initialism report,[102] the implementation of Sentinel as an automated transaction monitoring solution is broken into three phases:

(a) Deploy initial set of rules into production.

(b) Retune initial set of production rules and deploy RBA into production.

(c) Develop and implement additional automated transaction monitoring rules.

7.6.2 The first phase of the Sentinel implementation began on 2 February 2021 through the deployment of 17 RBA Sentinel Rules and seven large cash transaction Sentinel Rules.

7.6.3 The decrease in patron activity as a result of COVID-19 restrictions has meant the data required to assess the effectiveness of the Sentinel Rules has taken longer than expected. It is expected that within the next 6 months a review can be undertaken to assess the effectiveness of the phase one rule set.

7.6.4 When asked on what basis the effectiveness of a rule would be assessed, [redacted] did not provide a clear process but said it would include individual rule trigger rates, UAR/SMR submissions based off the alerts and comparison with manual transaction monitoring which will continue in parallel until Sentinel implementation is considered complete.

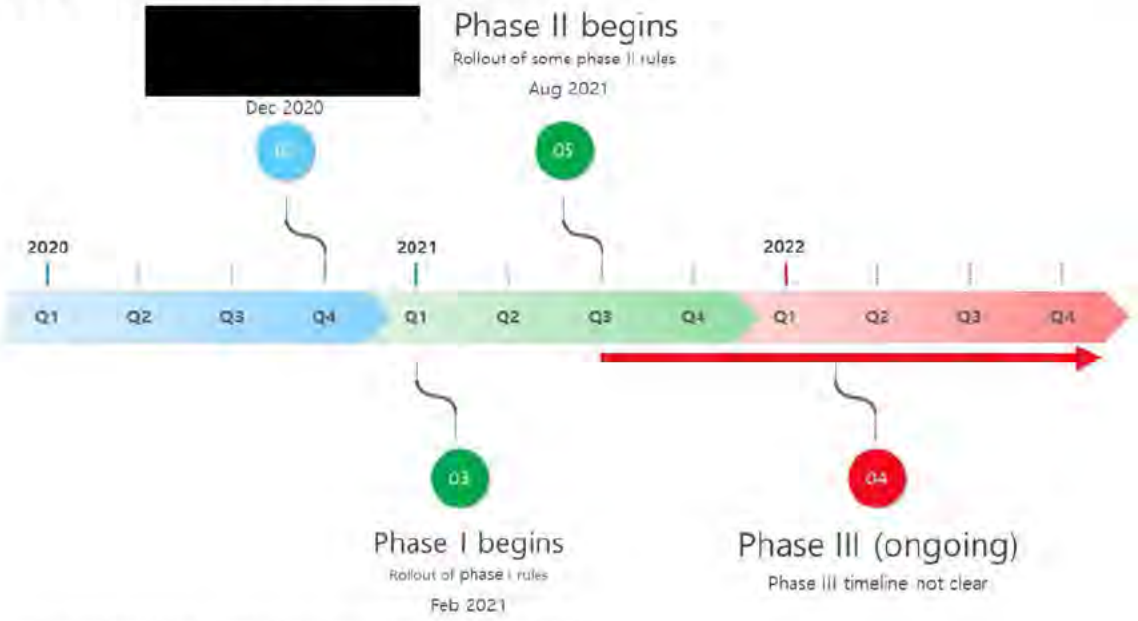
7.6.5 According to [redacted] feedback from the investigations team has already provided Crown with adjustments to be made to the current ruleset.

7.6.6 The Sentinel team states that they are also concurrently working on the production rules planned for phase 2 (b) with plans to deploy these rules into production in the coming months.

7.6.7 The timeframe for implementation of the full rule set is unclear. The estimated timeline for the implementation of the proposed Sentinel Rules is outlined in Figure 7 below:

[102] CRW.512.072.0128 Initialism Crown Resorts Transaction Monitoring Report

Figure 7. Estimated timeline of Sentinel implementation



Source: McGrathNicol, based on discussions with Crown staff

7.7 Findings

7.7.1 The program to develop an automated solution to monitoring activities for AML/CTF risk began in response to recognition that the manual reviewing was onerous and error prone.

7.7.2 The decision to use a centralised analytics engine (Splunk) receiving data from numerous sources within the casino in a format that allows many data sources to be considered in a single rule positions Crown well to develop a complete automated transaction monitoring program.

7.7.3 The quality and robustness of any analytics program is only as good as the data it receives. There are a number of risks associated with the current data inputs, particularly the manual and complicated nature of SYCO and the lack of transparent quality control processes associated with the ingestion of data.

7.7.4 Assurances have been given that improving the quality of data from these systems is an on-going process by the Sentinel team.

7.7.5 The program is in its infancy and the lack of operational data at the Melbourne location prevents an assessment of completeness of the phase one-rule deployment.

7.7.6 The overall project requires significant ongoing investment in human resources in addition to technological resources.

8 KYC processes

8.1 Overview of obligations for KYC

8.1.1 Under Division 4 of the AML/CTF Act, a reporting entity must carry out applicable customer identification procedures before providing designated services.[103] The applicable customer identification procedures, known as 'Know Your Customer' or 'KYC' processes are to be documented in Part B of an entities AML/CTF Compliance Plan. The reporting entity must be satisfied, through the application of KYC procedures that the individual with whom they are dealing is who they claim to be before providing a designated service.

8.1.2 Part B of the AML/CTF Program must include the following:[104]

(a) How the reporting entity collects and verifies KYC information;

(b) How the reporting entity identifies customers who are politically exposed persons (**PEP**s);

(c) How the reporting entity responds to discrepancies in verification information collected; and

(d) The risk-based systems and controls the reporting entity uses to work out whether they need to collect and/or verify further customer information.

8.1.3 For individual customers the minimum initial identification requirements, of which 2 must be verified, are:

(a) Full name;

(b) Residential address; and

(c) Date of birth.

Ongoing Customer Due Diligence

8.1.4 In addition to initial customer identification and verification Division 6 of the AML/CTF Act 2006 requires reporting entities to conduct 'Ongoing Customer Due Diligence' (OCDD).

(a) OCDD ensures the information the reporting entity has on an individual is up to date and ensures the customer assessed risk level is appropriate on an ongoing basis.

(b) The processes and procedures for conducting OCDD are in Part A of the AML/CTF program.

Enhanced Customer Due Diligence

8.1.5 Based on the outcomes of OCDD, transaction monitoring and risk assessments, ECDD may be required. Part A of an AML/CTF program must include an ECDD program that documents the actions taken if a customer's risk rating for money laundering and terrorism financing is assessed as moderate or higher.

8.1.6 ECDD may include requiring further identification checks to be completed on an individual, conducting open source research into an individual's background and gaining knowledge surrounding their source of funds / wealth. ECDD must be applied in the following high-risk situations:[105]

(a) When the risk of money laundering or terrorism financing is assessed as high;

(b) The designated service is being provided to a PEP or relative of close associate of a PEP;

(c) The customers suspicious activity may lead to making a SMR; or

(d) A transaction involves a person or company that has a presence or is incorporated in a prescribed foreign country.

---

[103] https://www.legislation.gov.au/Details/C2020C00362

[104] https://www.austrac.gov.au/business/how-comply-and-report-guidance-and-resources/customer-identification-and-verification/customer-identification-know-your-customer-kyc

[105] https://www.austrac.gov.au/business/how-comply-and-report-guidance-and-resources/amlctf-programs/enhanced-customer-due-diligence-ecdd-program

8.2 KYC at Crown

8.2.1 Crown's KYC framework, including policies and procedures, is set out within Part A and Part B of Crowns Joint AML/CTF Program.

8.2.2 Part A of the Joint AML/CTF Program focuses on the following topics:

(a) Customer Risk Assessment (Section 3)

(i) All customers that Crown provides a designated service to are allocated a risk level of either standard, moderate, high or critical. The risk rating is determined based on several rules outlined in the policy.

[redacted]

(iii) The customer risk rating is determined through the initial KYC process, OCDD or ECDD. Customers who are identified as PEP's or RCA will be assigned a higher risk rating. Transaction monitoring for unusual behaviour or previously lodged SMR's will be taken into account when assessing a patron's risk rating.

(b) Ongoing Customer Due Diligence – Transaction Monitoring (Section 6)

(i) Crown has implemented both automated and manual transaction monitoring procedures. The procedures may trigger alerts based on a range of rules such as customer activity / transactions. If these rules or alerts are triggered further due diligence may be required and the customers risk rating is re-assessed.

(c) Ongoing Customer Due Diligence – Review and update of KYC information (Section 7)

(i) This section outlines the processes in which new and active customers are screened daily against the Dow Jones Risk & Compliance product to identify changes in customer behaviour or the release of new information which may trigger further investigation or re-assessment of the customers risk rating.

(d) Enhanced Customer Due Diligence (Section 8)

[redacted]

(e) PEPs

(i) This section provides Crown's overview of PEP's, identification of PEP's and their procedure with dealing with them.

8.2.3 Part B of the Joint AML/CTF Program focuses on the following topics:

(a) The process in which Crown conducts customer identification.

(b) As a Casino, certain exemptions apply to Crown regarding identification of patrons; these exemptions are:

(i) Crown is not required to identify a patron where the designated service involves an amount of less than A$10,000;

(ii) Crown is not required to identify a patron where the designated service involves an amount of A$10,000 or more and the transaction relates to the giving or receiving of only gaming chips or tokens; and

(iii) Crown is not required to identify a patron where the designated service it provides to the patron involves an exchange of one currency for another for the value of less than A$10,000.

(c) In identifying a patron Crown collects at a minimum the following information:

(i) The customer full name including middle name

(ii) The customers date of birth; and

(iii) The customers residential address.

(d) To complete the customer identification process Crown must verify:

(i) The customers full name and either;

(ii) The customers date of birth; or

(iii) The customers residential address.

(e) Crown collects the above information about their customers via different means; these include:

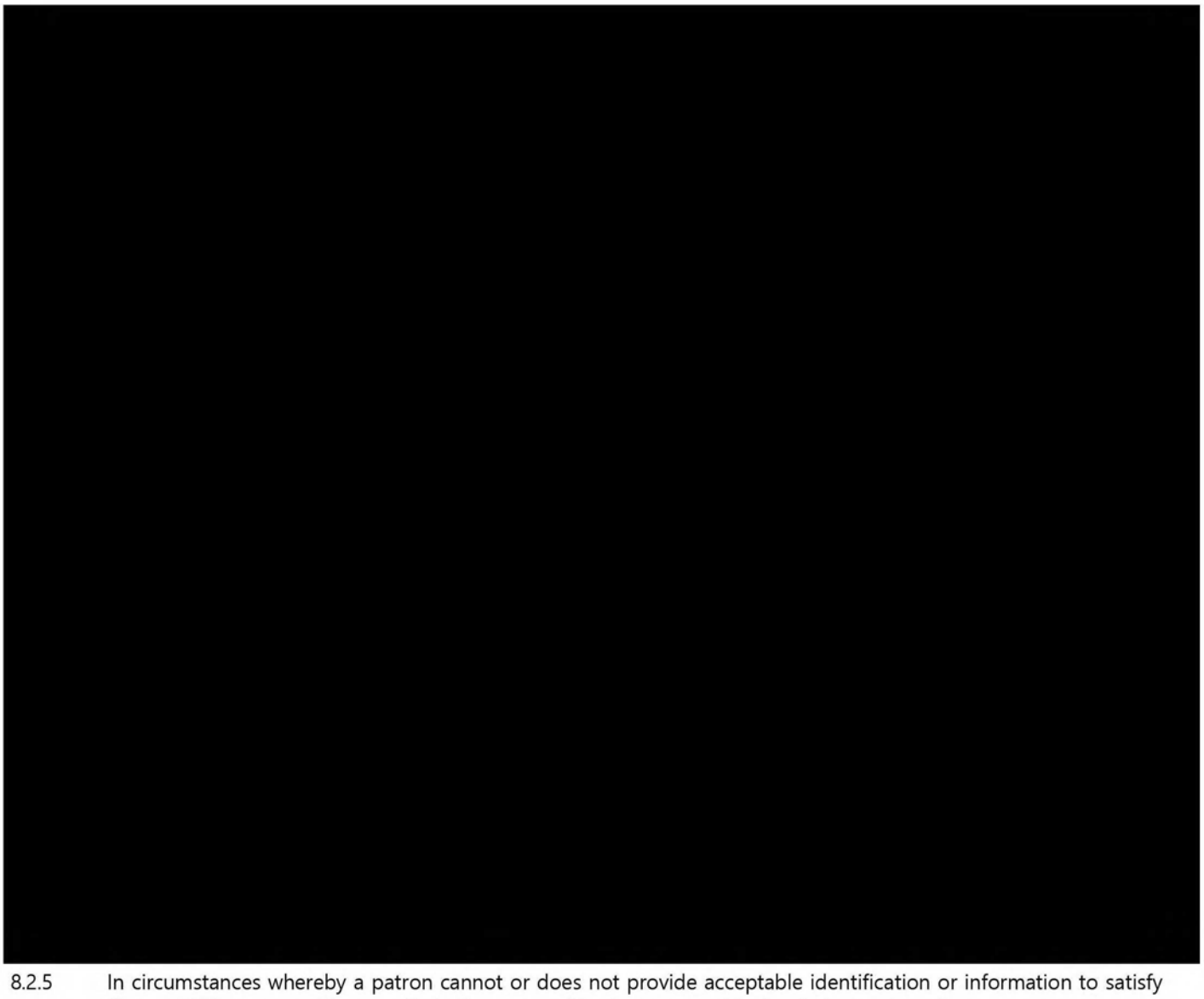
(i) Onsite

(ii) Member sign up application

(iii) Online; or

(iv) The Cage.

8.2.4 To be a key player, international program player, junket operator or junket representative, identification procedures will only be required to be conducted if the patron is transacting $10,000 or above.



8.2.5 In circumstances whereby a patron cannot or does not provide acceptable identification or information to satisfy Crowns KYC processes Crown will decline to provide the patron with the designated service.

8.3 Crown Rewards card and KYC

8.3.1 The loyalty program through which members can earn points to redeem for goods and services (**Crown Rewards**) is critical to Crown's KYC program. To obtain a Crown Rewards card and become a member, identification is required including such details as providing identification documents, full name, address, and date of birth.

8.3.2 When a patron approaches a table game, they are asked by the croupier if they have a Crown Rewards card. If the patron produces a Crown Rewards card this card is swiped by either the croupier or area manager and the patron will earn Crown Rewards based on the game they are playing (e.g. average bet for that table, average rate of play per hour and time spent gaming). Crown Rewards cards are also used on electronic gaming machines. This is known as "rated" or "carded" play which allows the Cage to identify cash outs as verified or unverified, based on the relationship between recorded transactions and ratings.

8.3.3 Along with providing the patron with rewards, the Crown Rewards card plays an integral role for Crown staff in identifying the patron and tracking their activities throughout the Casino.

8.3.4 Crown Rewards cards are required to access certain areas of the Casino. Patrons must be a Crown Rewards member and produce a Crown Rewards card to enter VIP rooms such as the Mahogany room or Teak room. On entry, the patron must provide their Rewards card, which is scanned showing the host a copy of the patrons ID and their relevant details. This enables Crown hosts to determine if the patron is who they are claiming to be.

8.3.5 During the focus groups conducted by McGrathNicol employees identified that the risk of money laundering and terrorism financing would be reduced if all patrons were required to have a Crown Rewards card in order to game. Focus group participants also commented that this might not be possible due to the amount of casual gamers that attend Crown, unwillingness of many customers to provide information about themselves and commercial pressures which come into play. Broadly speaking, the AML, Surveillance and Cage & Count teams were keen on compulsory cards, the gaming teams, less so.

8.3.6 Crown employees also noted that patrons with Crown Rewards cards often do not use them when gaming. This provides a challenge for Crown staff to determine what gaming has taken place and whether the cash out / winnings are verified. Staff noted that patrons don't use their Crown Rewards cards for a number of reasons including:

(a) Superstition surrounding the card being bad luck;

(b) Not wanting their gaming to be recorded; or

(c) To avoid responsible gaming restrictions.

8.4 Bergin report findings

8.4.1 The Bergin report identified potential deficiencies in Crown's KYC procedures based on correspondence between Crown and its bankers ANZ and CBA when those banks had raised concern about Crown's KYC processes in 2018 and 2018 respectively.

8.4.2 ANZ made the following comments regarding Crown's KYC practices on 5 March 2015,[106] after which no changes were made to the operation of the Southbank or Riverbank accounts:[107]

(a) "It appears only minimum information is obtained for patrons including name, DOB and residential address. For ANZ the minimum collect requirements per [customer] is name, DOB, address, occupation, Citizenship/Nationality for individual customers."

(b) "...there is no evidence of client review or rejection/exit from adverse media, sanction or PEP related notifications where these would be deemed above Crown's risk appetite."

(c) "Risk rating of customers is automatically set at "Low" unless or until the AML/CTF Officer or Cash Transaction reporting Manager decides to elevate the customer risk rating, which would not be re-assessed for another 2 years", which they suggest is too infrequent.

(d) "Crown's CDD is not aligned to ANZ's customer risk rating requirements..."

8.4.3 The Bergin report also outlined Crown's responses to queries from CBA on 20 December 2018 which stated that "Under Crown's AML/CTF Program, Crown conducts the KYC checks – identification and face-to-face verification against Primary ID provided by the customer – in advance of accepting an outbound instruction from a customer and/or before providing funds to the customer on an inbound instruction...In addition, Crown uses the Dow Jones Risk & Compliance product to screen all active customers to detect if the customer is a PEP/sanctioned/on a watch list..."[108]

8.5 Policy and process changes

Significant Player Review

8.5.1 As at 12 March 2021 [redacted] drafted the "Significant Player Due Diligence Policy"[109] which was approved by Xavier Walsh (CEO). This policy supports Crown's KYC and OCDD processes through providing guidance and framework to assess customers who trigger certain thresholds. The policy is designed to identify high-risk customers who may be escalated for ECDD and/or review as to whether Crown wishes to continue its relationship with the patron.

---

[106] As reported by Bergin (section 3.2 paragraph 58) in relation to comments made by ANZ regarding the Promontory Report findings

[107] Bergin Inquiry - Section 3.2 paragraph 60

[108] Bergin Inquiry - Section 3.2 paragraph 86

[109] CRW.512.073.0332 - Crown Resorts Limited – Significant Player Due Diligence Policy

8.5.2 The Significant Player Review (**SPR**) process is summarised as follows:

(a) A representative of Table Games and Gaming Machines will implement first line due diligence in relation to significant players or customers who trigger certain defined thresholds as set out in the policy within defined time periods. The purpose of the due diligence and review is to identify risk factors whereby an individual's rated play is inconsistent with their source of wealth.

[redacted]

[redacted]

8.5.3 On 21 May 2021 Nick Weeks (Executive General Manager, Transformation & Regulatory Response) reported to the Board[110] that reviews had been undertaken across all three Australian Crown properties including completed reviews for more than 1,320 top customers in Melbourne and more than of 30 Sydney based customers who are expected to become Crown Sydney customers.

8.5.4 Of the customers who have been referred to the POI committee 198 have been issued with a WOL for failure to provide sufficient source of wealth information. A further 43 customers are awaiting decision by the POI committee.

8.5.5 These results clearly indicate a tightening of the KYC policies and procedures and a preparedness to cease business with customers who do not meet Crown's KYC requirements or are found to be an unacceptable risk.

*Source of Funds (**SOF**) Policy*

8.5.6 In December 2020 the "Source of Funds (SOF) Form – Cash transactions policy"[111] was issued. This policy requires employees to have the customer complete an SOF form for all cash presented once prescribed daily cash limits are reached and to report the transaction via a UAR to the AML Team.

8.5.7 The prescribed daily limits as stated in the original policy were as follows:

(a) Cash presented up to $49,999 for a calendar day would cause a TTR to be completed as usual and a UAR may be completed if the staff member deems it appropriate.

(b) Cash presented for a calendar day between $50,000 and $149,999 requires a SOF form to be completed by the Cage manager. A TTR entry is to be made. A UAR along with the SOF form must then be forwarded to the AML Team.

(c) Any single cash buy in for $50,000 or more at a table location will be referred directly to the Cage for completion.

(d) Any single cash transaction or accumulated total of cash presented on a calendar day between $150,000 and $200,000 will cause a SOF to be completed by the Cage or Table Games representative which must be approved by the COO or CFO and either the Group AML Compliance Officer or the Group GM Risk and Audit Manager.

(e) Cash amounts presented for a single calendar day that exceed $200,000 are not permitted and will not be accepted in any circumstances. This includes accumulated cash transactions which may exceed the limit.

8.5.8 The daily cash limit has subsequently been reduced to $25,000.

8.5.9 The SOF requirement augments Crowns KYC processes as it requires staff to obtain additional information and give consideration to the source of funds stated so as determine whether the funds are acceptable for gaming purposes.

8.5.10 The SOF form requires the patron to stipulate from where the cash presented has been obtained. If the information provided is not plausible or is incomplete the transaction must be escalated through to Senior Management before proceeding.

8.5.11 Focus group participants noted the implementation of the SOF policy has added extra controls to the Casino floor and has caused many cash transactions to be declined. Comments from focus group participants included:

'The SOF / SOW requirements and thresholds have added extra controls to the Casino floor (currently a SOF form will be required where a customer attempts to buy-in more than $25,000 in a single transaction or more than $25,000 in a single calendar day where each transaction is at least $10,000 and would therefore require a TTR to be completed.'

---

[110] CRW.512.110.0060

[111] CRW.709.063.1664

'Currently around two out of three SOF forms are rejected by Cage cashiers as they don't satisfy the requirements e.g. 'given money by a friend' or 'bank loan' in which case the buy-in transaction is not completed.'

"Before, we didn't have limits...we would be keeping an eye on it ourselves and then obviously there would be an investigation when the amount got crazy...but now we have the source of funds..."

"Since the Bergin Inquiry we've now gone to having a policy where they must actually declare where the money's from...above a certain threshold...and I would say probably 2 out of every 3 are probably rejected."

Identification digital verification system (DVS)

[redacted]

FCCCP KYC Initiatives

8.5.15 The FCCCP board pack[112] provides a high-level controls uplift roadmap involving the following elements which include assessing risk and advancing capability and effort commensurate with risk. The timeline for completion is shown in Figure 9 and summarised below.

(a) By December 2021:

[redacted]

(b) In 2022:

[redacted]

[112] CRW.512.081.1750

Figure 9

Source: CRW

8.6 KYC challenges and risks – according to employees

8.6.1 KYC / due diligence (**DD**) challenges noted by Crown Employees included:[113]

(a) Crown is limited in the amount of information they can collect on customers and have less access to information than banks do.

(b) Crown is limited to external reports and publicly available information.

(c) The second line AML team currently have resource constraints and competing priorities.

8.6.2 Additional information or capabilities suggested by Crown staff to improve KYC and DD procedures included:[114]

(a) Receiving more information from law enforcement to enable Crown to identify potential bad actors before they entered the premises or started gaming.

(b) Facial recognition across all tables would allow alerting surveillance a lot easier and quicker.

(c) Currently KYC and DD processes in place are extremely manual; staff must collate customer information from a range of different databases / systems. A one-view complete customer source would make this process more efficient and effective.[115]

8.6.3 The following are quotes obtained by McGrathNicol through focus groups, interviews, and questionnaires:

"I am certainly aware that a significant number of high end patrons have been exited from the business since Crown has adopted a very different attitude towards source of wealth requirements – that is, Crown commenced a process of 'Know your customer' which is in my time unprecedented. I would say the culture of Crown has changed from wealth focus to a compliance focus." Craig Walsh (Executive Director Security and Surveillance), Questionnaire response

"There is no doubt that there's been a push back to the departments...to make sure that they look at these obligations more strongly, so each of the departments, whether it's gaming machines or Table games or Cage...have to look at their customers...they have to look at their more predominant players, usually it's their higher-tier customers, but there is a push to know their customer and they keep records of whatever information they can put together, of which the AML team can use." Focus group participant

"That's why you have to know your customer...so it's easy to approach them...if you build the relationship it's easy to talk to them." Focus group participant

"Once you go to silver, or go up a tier, every six months... on the first of October and on the first of April they have to come to Crown to renew the card again." Focus group participant, explaining how Crown has an opportunity every 6 months to re-validate KYC data.

---

[113] Interview with [redacted]

[114] Interview with [redacted]

[115] Interview with [redacted]

9 Financial Crime and Compliance Change Program (FCCCP)

9.1 About the FCCCP

9.1.1 The FCCCP is a roadmap for significant development and change in Crown's financial crime and compliance program over the period to December 2022. It was developed by Mr Blackburn, Group Chief Compliance and Financial Crime Officer and approved by the board on 24 May 2021. Mr Blackburn is responsible for its implementation.

9.1.2 In a memo to the board dated 24 May 2021 Mr Blackburn said of the FCCCP:[116]

To effectively manage financial crime risk and the associated regulatory risk, Crown must continue to evolve the financial crime program through material and ongoing investment in capacity, capability and technology.

In its current state, Crown's compliance program, meets regulatory requirements but the compliance function is under resourced and is not adequately supported for regulatory change and responsiveness. As with the financial crime program, Crown's compliance program requires considerable investment in order to improve and evolve.

The FCCCP seeks to build on Crown's existing financial crime and compliance foundations introducing changes that will ensure the stability of the two programs whilst industrialising and optimising the functions wherever possible.

9.1.3 The memo refers to key actions and outcomes and notes:

To be successful each of the foregoing changes require the commitment engagement and support of the whole organization and the Board, as well as committed funding for the longevity of the FCCCP. The proposed changes will also have implications for other Crown functions including Technology, Operations, Surveillance & Security, Procurement and Human Resources. While none of the proposed changes can alter Crown's past exposure to financial crime and compliance risk, they will assist Crown in reducing its future risk.

9.2 Appointment of Mr Blackburn as Group Chief Compliance and Financial Crime Officer

9.2.1 McGrathNicol interviewed Mr Blackburn on 3 June 2021 and the commentary in this section of the report is based on the information provided by Mr Blackburn in that interview and documents as referenced.

9.2.2 Mr Blackburn was appointed on 24 February 2021 after being approached by a recruitment firm in October 2020.

9.2.3 Mr Blackburn advised McGrathNicol that he was attracted to the role at Crown because it offered the opportunity to do what he had done before in building out a modern financial crime program, but it also offered greater breadth of responsibility across compliance and responsible gaming.

9.2.4 Before agreeing to take up the position with Crown Mr Blackburn asked to meet with a number of board members in order to assess their desire to make change and gain comfort as to the preparedness of Crown to make real change. Having satisfied himself through these conversations and obtaining assurance from Peter Barton, then CEO, that his mandate to help build out a modern financial crime would be supported, he resigned from his position at National Australia Bank (**NAB**).

9.2.5 After training and practising as a lawyer, Mr Blackburn has more than 10 years in senior financial crime risk and operations roles in the banking sector in Canada and Australia. Mr Blackburn was the Chief Anti-Money Laundering Officer at the Canadian Bank of Commerce from January 2011 before being recruited by National Australia Bank to come to Australia and take up the role as Chief Financial Crime Risk Officer and Group Money Laundering Risk Officer.[117] Mr Blackburn does not have previous casino experience.

9.2.6 Mr Blackburn described his mandate at Crown to McGrathNicol as:

[116] CRW.512.081.1791 Memo to Board 24 May 2021

[117] Statement of Steven Blackburn to RCCOL 21 April 2021

Financial Crime

(a) To build and maintain a financial crime program that is commensurate with the risk that Crown faces in providing designated services to the public.

(b) To ensure that the financial crime program meets regulatory requirements but also regulatory expectations, as well as his expectations of Crown's role in Australia's financial crime eco-system.

Compliance

(c) To ensure that the compliance policies and approaches are appropriate for the organisation and to change the policies where necessary in order to comply with relevant legislation, rules and licencing requirements.

Responsible Gaming

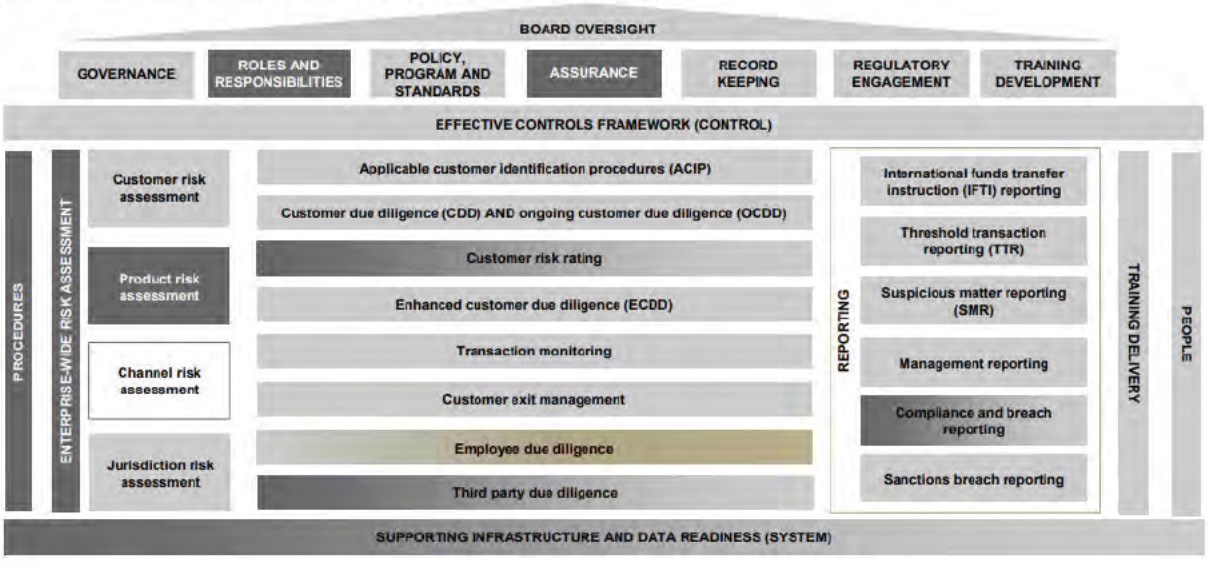
(d) To consider and develop strategies to enhance Crown's responsible gaming approach and run the program on an ongoing basis.

9.2.7 The FCCCP is the roadmap for development of the financial crime and compliance programs to achieve an advanced level of maturity by December 2022.

9.3 Financial Crime and Compliance (FC&C) maturity – current state

9.3.1 As part of his development of the FCCCP, Mr Blackburn undertook an assessment of the current state of maturity of all the elements which contribute to a financial crime program and presented the assessment pictorially as a "house" in which the various elements were colour coded to represent his assessment of the maturity of each element. This pictorial is shown in Figure 10.

Figure 10 Current state maturity (31 May 2021) as assessed by S Blackburn



Key:

Source: CRW.512.081.1750

9.3.2 The elements of a financial crime eco-system addressed by Mr Blackburn is comprehensive and consistent with regulatory requirements. The assessment has been made as at 31 May 2021, and accordingly is inclusive of a number of changes which had been implemented in recent months including:

(a) Approval of Joint AML/CTF Program on behalf of the designated business group in November 2020;

(b) Increase in FTE in Financial Crime team from 5 to 20 between December 2020 and May 2021;

(c) Engagement of Promontory to conduct a review of AML vulnerabilities to inform an enterprise wide risk assessment yet to be undertaken. Draft report delivered 29 March 2021 and final report delivered 24 May 2021;

(d) New automated transaction monitoring program, Sentinel, launched 2 February 2021;

(e) New Unusual Activity Reporting regime launched 12 April 2021;

(f) Online financial crime awareness training released in early 2021 with 90% completion rate; financial crime training provided to Board March 2021;

(g) Cessation of Crown dealing with junkets;

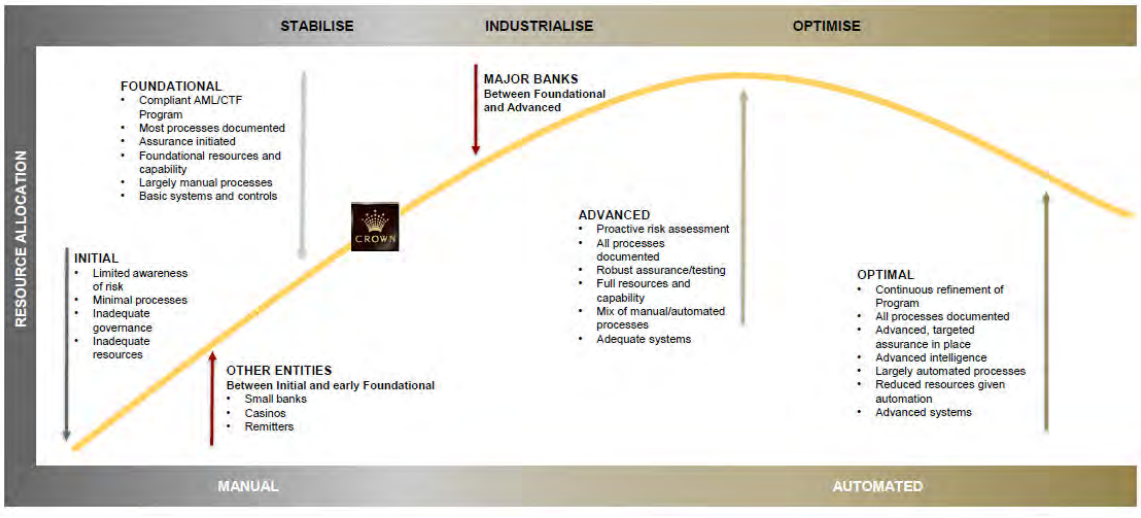
(h) Source of funds declaration requirement for all customers depositing >$25,000 cash in a day introduced from 21 May 2021; and

(i) A number of patron account controls introduced which Deloitte assessed as being effective but with sustainability risk as casino activity increases post COVID-19 (as discussed in section 4).

9.3.3 Inclusive of these considerable developments, Mr Blackburn assesses the maturity of the FC&C system overall as "foundational" with a number of components in transition to that stage from "initial". But for these recent developments, more elements of the FC&C eco-system would likely have been assessed as "initial" and it would be difficult to support a view that overall the system could have been assessed at a maturity level greater than "initial".

9.3.4 Figure 11 is a copy of the "Financial crime Eco-system maturity arc" diagram which Mr Blackburn included in his presentation to Board on 24 May 2021.[118]

Figure 11



Source: CRW.512.081.1750

9.3.5 This diagram includes Mr Blackburn's descriptors of the stages of maturity from "Initial" to "Optimal" and each position on the arc shows the relationship between the resources invested across the spectrum from manual to automated processes (lower horizontal axis). As a system matures to the "Advanced" stage, increasing resources are required to develop, implement, automate and thereby and institutionalise or industrialise policy and procedures. Thereafter, the resources required diminish as much is cemented into core business functions and the focus is on emerging issues and ongoing assurance.

9.3.6 Mr Blackburn has placed the Crown logo on the curve in the position he assesses Crown to be, a position he describes as "foundational" overall, with some aspects remaining "initial". We queried Mr Blackburn on the following aspects of his diagram:

(a) The pictorial representation suggests that Crown is beyond "Foundational" and on the way to "Advanced".

[118] P4 CRW.512.081.1753

(i) Mr Blackburn's response was that he was surprised (based on what he'd heard in the media or from the Bergin Report) that Crown had already progressed to a "Foundational" stage in regard to its controls.

(ii) When he started at Crown, there were already controls in place to address material risks which could be built on going forward.

(iii) The primary reason for the "Foundational" assessment was their extensive employee due diligence processes. Licencing regimes apply scrutiny to each individual hired by a casino, which require the individual to go through invasive processes to become licenced.

(iv) In addition, each prospective employee goes through Dow Jones screening assessments (which also occurs daily for existing employees), media assessments and police checks. Mr Blackburn's opinion was that these processes are more robust than those of most reporting entities in Australia.

(b) Mr Blackburn represents the major banks as not so far ahead of Crown and well short of "Advanced".

(i) Mr Blackburn's advised that it was difficult to categorise all the major banks as a group, with some banks being closer to "Advanced" than others.

(ii) In comparing casinos to the banks, Mr Blackburn expressed the views that:

- There are a lot of variations and complexities in the banks such as the type of ways that customers can come in (e.g. trustees, beneficial owners of corporations, etc.) which potentially makes identifying risks clearer in a casino than in a bank.
- Crown is currently similar to where the banks might have been 20 – 30 years ago.
- Banks do not have processes for screening their employees that are as extensive and invasive as casinos, citing the vetting processes involved in his obtaining a Special Casino Employee Licence.

9.3.7 A number of the elements of the FC eco-system which Mr Blackburn has assesses as of "initial" maturity are set out in Table 13 together with comments from Mr Blackburn as he elaborated on his assessment in our interview.

Table 13

Element	Additional comment and basis for assessment by Mr Blackburn	McGrathNicol view
Enterprise wide (ML/TF) risk assessment (**EWRA**)	Risk assessments have been undertaken for discrete or different categories of risk including financial crime risk, but what hasn't been done is an end-to-end enterprise wide entire risk assessment of financial crime. An EWRA has been commissioned and is aimed to be completed by end of 2021. It is a significant task and requires going deep into each category of risk e.g. customer risk, product risk assessment (EGM v Table games), jurisdictional risk. The work done by Promontory into vulnerabilities to ML is only one aspect of risk.	Mr Blackburn's observations on the nature of Crown's AML risk assessments is in accordance with our observations and the documents available to us. We also agree that to undertake the process in a robust manner – sufficient to support a substantial AML/CTF Program and risk mitigation and management framework - is a significant piece of work which requires input from a wide range of people.
Procedures	They call them procedures, but they consist of some policies, guidelines and work instructions. There is not a clear hierarchy around compliance or financial crime frameworks. It is currently difficult to figure out where they are and what to do with them. They need to clarify the procedures and ensure that there is an appropriate framework so that first line staff (in particular) can access them and understand what their responsibilities are.	Mr Blackburn's comments are consistent with our observations of the documentation of policies. Policy / procedures appears to be issued in EOMs, Corporate Policy Statements, AML/CTF Policy Statements , AML/CTF Rules, Guidelines and across the Part A and Part B AML/CTF Program as well as Statements of Procedures.

Roles and responsibilities	The roles and responsibilities are in a state of transition. The organisation is coming to an understanding of the concept of the three lines of defence model but it is still relatively fresh and they are not yet at the stage where it has been "elegantly documented". They need to document the processes so that employees from each line of defence know what their roles and responsibilities are in relation to financial crime and what to expect of others in different lines of defence. Blackburn is also currently developing a Responsible Accountable Consult or Inform document (RACI) so that everyone understands "who's on first". There really hasn't been a second line of defence and the first line has understood its obligations more in a procedural sense rather than with a deep understanding of the responsibility they carry in protecting the vulnerable from financial crime.	Mr Blackburn's comments are consistent with our observations. We were unable to procure a settled organisation chart and when we selected people to respond questionnaires or attend interviews we encountered by reference to their title, we encountered instances of the employee having only just moved to that role and not yet clear on the organisational structure or their full job description.
Assurance	The second line function in operation was minimal. There was activity in the manner of gaming auditors who would test compliance of employees in implementing gaming rules and procedures. But that was the extent of the assurance activities, and it did not extend to specific AML/CTF controls assurance. The third line were applying some oversight, however Blackburn noted that in his experience the third line might not be experts in financial crime as they are usually generalists, so it is the second line's role to provide assurance that financial crime risks are being managed and mitigated effectively. There will be redeployment of existing employees with casino specific experience, as well as the addition of proposed recruits, to introduce an effective second line of defence or assurance function.	Mr Blackburn's assessment is consistent with the information we have reviewed and otherwise gathered in the course of our work. We have seen no evidence of systemic review of the effectiveness of controls, bar the engagement of Deloitte to undertake such a review in Phase 1. An internal audit team member involved in the focus group confirmed that AML/CTF controls were not within scope of the internal audit plan.
Supporting infrastructure and data readiness (systems)	Data readiness remains a challenge. The current systems are heavily manual; a key element of his FCCCP is to introduce automation so that the humans can focus on matters that are not routine and require skills and experience. Mr Blackburn noted that is difficult to obtain data for transactions involving less than $10,000 because of the exception in the AML/CTF Act, and they often have to piece together information from the surveillance system. Mr Blackburn also noted that they have really good technology partners in the business and some of the best tech people that he has ever met, so he will be able to leverage existing talent in the tech space. He also noted that there are no off-the-shelf systems for financial crime and casinos so this requires highly skilled tech staff to build their systems.	Crown has substantial technology infrastructure and capability, including an IT team of some 180 FTE. The technology is visible on the casino floor in the form of security, surveillance, automated gaming and data capture via membership cards. It would appear that the capability has been developed for and directed towards priorities other than AML/CTF and to the extent it supports AML/CTF functions, it has been more by coincidence than design.

9.3.8 No elements of the financial crime eco-system were assessed by Mr Blackburn as being "optimal" meaning that they are fully operational, robust and implemented efficiently.

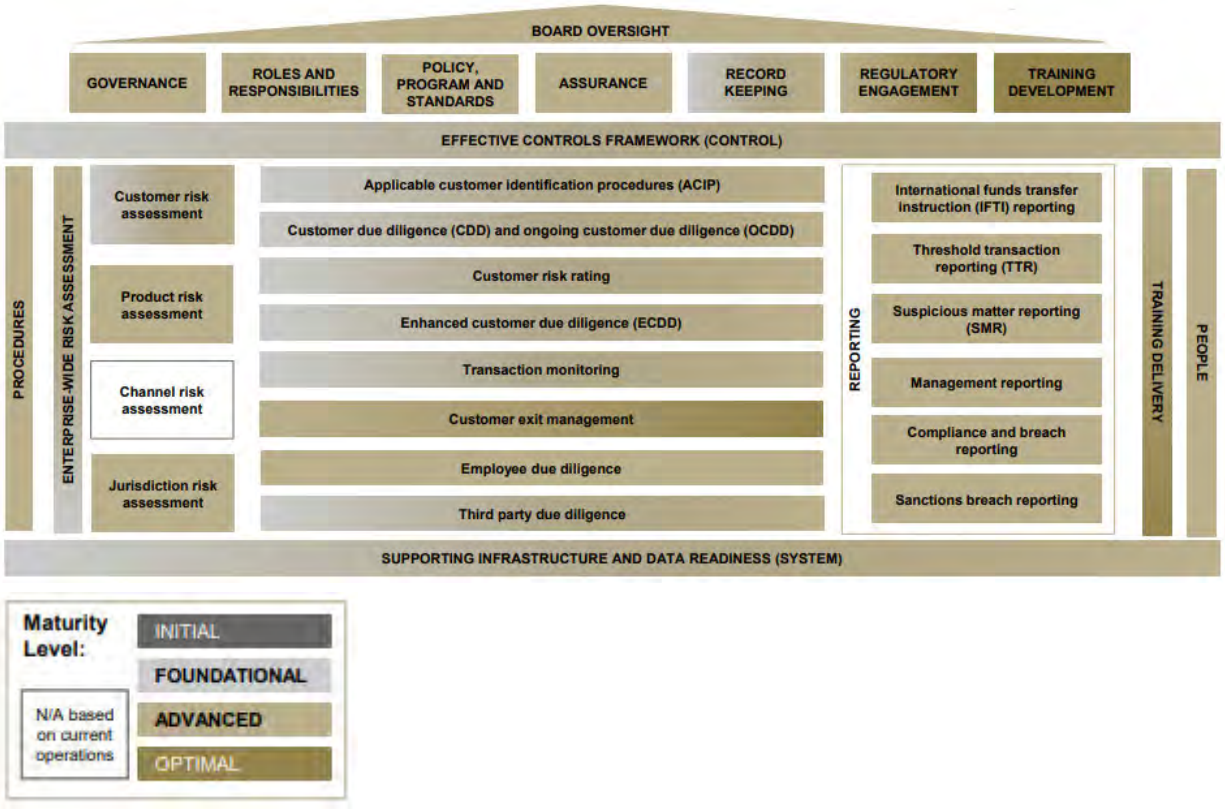
9.3.9 Mr Blackburn points out, correctly in our opinion, that it is not necessary that every element be at an optimal level, that this is a matter for cost benefit determination with reference to the assessed risk addressed by each element. Notwithstanding, in our assessment it is a serious indictment on Crown's focus on and investment in AML/CTF over its life, and particularly since the AML/CTF legislation was introduced in 2006, that Mr Blackburn assesses the AML framework overall as "foundational" and that many elements are not assessed at even this level of maturity.

Future State December 2022

9.3.10 The proposed state under the FCCCP is to be in an overall aggregate state of "advanced" maturity by December 2022 and Mr Blackwood represents the maturity levels at that time as shown in Figure 12.

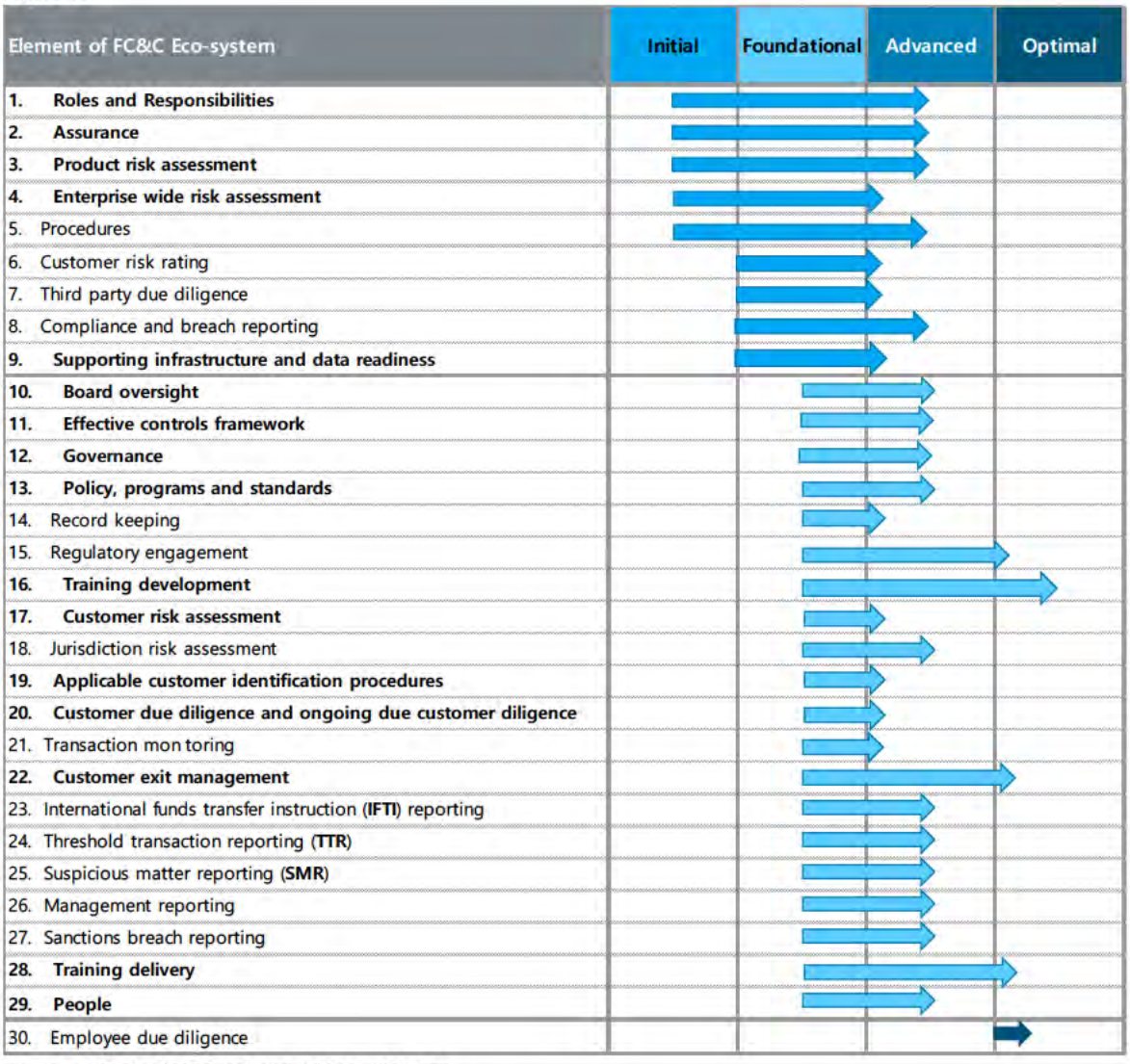
9.3.11 In Figure 13, we have tabulated each of the elements of the FC&C eco-system "house" and mapped the improvement proposed from current state to December 2022 state. The bold text highlights those elements which correlate to the ten key areas upon which the FCCCP will focus (refer 9.4).

Figure 12



Source: CRW.512.081.1750

Figure 13



Source p5 & 11 FCCCP Board deck CRW.512.081.1760

9.3.12 In our assessment, by any measure this is an ambitious plan, but, at the same time necessary if Crown is to comply with its obligations to have an AML/CTF Program which is risk based and commensurate with the size and complexity of the organisation, as required by the AML/CTF Act and Rules and if it is to ensure the management and operation of the casinos remains free from criminal influence or exploitation as envisaged by the Casino Control Act.

9.4 Overview of the plan

9.4.1 Mr Blackburn's memo to the board of 24 May 2021 itemises 17 key actions and outcomes. Figure 14 is an extract from the board presentation on the FCCCP within which the 17 key actions are consolidated into ten key areas for uplifting Crown's financial crime and compliance programs.

Figure 14

Source: CRW.512.081.1750

9.4.2 Mr Blackburn indicated that accountability has or will be assigned for each of these areas or key actions and a more detailed plan is to be developed to guide execution and assess progress. The balance of the board pack provides a high-level overview of significant aspects of the plan as summarised in Table 14. We comment on these proposals and the risks to implementation in section 9.5.

Table 14 Summary of FCCCP initiatives

Area	Changes proposed and approved by Board on 24 May 2021
People	▪ Reorganisation of the FC&C function into 6 specialist teams with clear functions – Financial crime Risk – Compliance & Regulatory affairs – Operations – Assurance – Solutions – Responsible gaming – Surveillance ▪ An increase of a further 54 FTE across all areas of the FC&C in addition to approximately 56 FTE already on-boarded or pre-existing bringing total FTE to 111 plus 10 FTE in temporary roles (largely change management) ▪ Remuneration uplift to market rates to attract and retain talent ▪ Proposed cost of $21.7m pa including on-costs ▪ Introduction of FC& related KPOs into position description and performance criteria for all employees with specific targets for executives
Risk Appetite	▪ Qualitative risk appetite statements to be articulated to frame the identification of metrics enabling measurement of performance and risk profile
Document framework	▪ Implement hierarchy of documentation flowing down from legislation and risk appetite statements through policy, to standards to operating procedures and processes

EWRA	▪ Redesign ML/TF risk assessment framework with contemporary approach, design and governance and better aligned with regulatory expectations that assessment is risk based and tailored to Crown ▪ Methodology to take into account 4 key risks: – Customer – Jurisdiction – Product – Channel
Reporting Governance	▪ Financial crime oversight committee formed to report to the Board ▪ Supported by a financial crime working group ▪ Augmented pro-active risk-focused reporting
Assurance	▪ Introduction of an effective second line of defence to assess and test compliance with policy and program obligations ▪ A 16 FTE team is proposed
Training	▪ Proposed shift from compliance focus to outcome focus training which prioritises the protection of the vulnerable from the impacts of financial crime ▪ Targeted training for high risk employees, senior management and the Board
Roles and responsibilities	▪ Development of a RACI (Responsible, Accountable, Consult, Inform) matrix to clarify the roles, responsibilities and obligations which fall to each line of defence and each accountable executive
Controls	▪ Continuation of the uplift of controls seen over the last 6 months including controls to address the vulnerabilities identified in the Promontory review
Data analytics & IT	▪ Enhancement, systems integration and analytics to improve quality and consistency of key functions – KYC, transaction monitoring, reporting ▪ Enhanced dashboard-based reporting of relevant metrics for key users ▪ Capture and use of data for assurance, risk assessment and intelligence gathering and insights ▪ Ongoing program of uplift and rationalisation of disparate systems
Surveillance	▪ Centralisation of function and implementation of standardised policies procedures, investigative approaches, law enforcement engagement, communications and reporting, recruitment and training, data capture and use

9.5 Dependencies and risks for implementation of the FCCCP

9.5.1 As noted above, in our view the FCCCP is ambitious and all the more so within an 18-month timeframe to deliver a substantially more mature FC&C system. Over and above the Board approved $21.7 million costs involved in doubling the already expanded financial crime and compliance team, the plan calls for support and commitment, backed by funding, from across the business and from the board down to the casino floor. As Mr Blackburn states in his 24 May 2021 memo to the Board:

To be successful, each of the foregoing changes require the commitment, engagement and support of the whole organization and the Board, as well as committed funding for the longevity of the FC&C Change Program.[119]

9.5.2 Further Mr Blackburn notes:

The proposed changes will also have implications for other Crown functions, including Technology, Operations, Finance, Surveillance & Security, Procurement and Human Resources.[120]

Technology support

9.5.3 We discussed the technology dependencies of the FCCCP with Mr Andre Ong, head of IT who advised:

(a) Mr Blackburn consulted with him and various members of his team in the process of developing the FCCCP and he is, and he believes all relevant decision makers are, aware that there will be demands on IT in relation to the FCCCP.

[119] CRW.512.081.1792

[120] ibid

(b) No specific budget has been established or committed to in relation to the FCCCP related IT requirements of which to date he has logged almost 40 projects, of varying size and complexity.

(c) While some of the projects are advanced in implementation (e.g. Sentinel, Unify for UAR automation) but many are proposals which have yet to be subject to:

(i) Discovery – ascertaining what is required and how it fits with existing systems; nor

(ii) Scoping – design and costing the development and implementation program.

(d) Mr Ong, in consultation with Mr Blackburn has estimated at a high level the uplift in capability and resources which would be required to deliver the requirements of the plan. He estimates an additional 29.5 FTE will be required across the 18-month period across a range of capabilities. This represents an increase of approximately 17% on current FTE, although not all will be brought on as employees; contractors will be used.

(e) Mr Ong advises it would not be typical to budget for the IT components of the FCCCP specifically. Rather, he indicated that "*everyone knows there is a placeholder for IT's uplift*" to accommodate the FCCCP. All IT projects are managed dynamically by planning the necessary resource based on scope and delivery dates and constantly updating for changes. If a new project comes on or there is a change in delivery dates or scope for example, the program loading tracker is updated and any mismatch between demand and supply is addressed by the business.

(f) There are several other major IT projects planned for the same period as the FCCCP, some of which align with the FCCCP. Other demands on IT in this period include:

(i) Technical Requirements Project in relation to the regulated systems

(ii) Anticipated opening of Sydney casino which will incorporate new and advanced technology which will then be replicated in the other casinos to continue the path of rationalisation of Crown's systems

(iii) Managing end of life for key systems such as security

(iv) Ongoing cloud transition for certain systems

(v) Supporting updates to Crown Rewards program including in relation to responsible gaming

(vi) Ongoing discovery processes to support cashless gaming

People risks

9.5.4 Mr Blackburn expressed confidence that he will be able to fill the many positions he has created. He has sought to create teams which include experienced casino staff and external recruits who are unlikely to have casino experience but will bring modern AML/CTF capability.

9.5.5 He had some concern about the ability to recruit given his assessment that the pay scale was below market and the brand damage Crown has suffered through recent months, but he believes that the commitment to market salaries, the opportunity presented to risk and AML specialists to be involved in a major change program and his personal brand will enable him to attract the talent he needs.

9.6 Key observations and assessment

9.6.1 Subject to the risks associated with the dependencies noted above, it is our assessment that it is likely that the FCCCP will give rise to a significant change in Crown's understanding of and performance in AML/CTF over the ensuing 18 months. We say this because:

(a) We consider that Mr Blackburn has the capability, track record and standing to lead such an ambitious program. Further, he is not burdened by the history of Crown's past underperformance and has the "fresh eyes' advantage by having subject matter expertise honed in a different sector, which enables him to question practices and ideas which may not be considered open to question by those only experienced in casinos.

(b) The FCCCP he has developed is comprehensive and in our view the areas of priority Mr Blackburn has identified are apt.

(c) Whilst the task is great, there is a rare window of opportunity over the next several months at least, as there has been for the last 6 months also, to embed new processes and practices which may be challenging to customers, in an environment of little international patronage and lower patronage overall.

(d) A number of significant control changes have already been implemented and appear to be effective, albeit it is difficult to measure in the current environment while the Casino is operating at low volumes and moreover is subject to intense scrutiny which would have staff on high alert and would be money launderers staying away.

(e) Our sense from the surveys we conducted and the focus groups held was that employees in the first line of defence are ready, willing and able to do what is asked of them when it comes to upholding the rules; but they do not make the rules and they rely on those that do to set them in accordance with Crown's values which includes "do the right thing".

9.6.2 Whilst we are of the view that an uplift in Crown's performance is likely, we consider there is considerable risk associated with achieving an advanced stage of maturity of the FC&C eco-system in the proposed timeframe due to the ambitious nature of the target, the dependencies and risks noted in section 9.5.

10 Money laundering "on the floor"

10.1 Risk of money laundering "on the floor"

10.1.1 As with all casinos the Crown Casinos are inherently at risk of facilitating money laundering due to the nature of the activities and services that they provide.

10.1.2 We have investigated the likelihood of money laundering activity being undertaken at Crown's Melbourne Casino at the current time by:

(a) considering in this section how Crown recruits and equips its first line of defence, the employees and business units responsible for the risks and for implementing the controls to manage and mitigate the risks; and

(b) engaging, by survey and focus groups, with Crown employees in the first line of defence, those who work on the Casino Gaming floors to gather their views as to the likelihood of ML/TF activity at Crown currently and how they contrast the current situation to that which prevailed prior to COVID-19.[121] The results of the surveys are in section 12 and the output from the focus groups is in section 13.

10.2 The First line of defence

10.2.1 The first line of defence (**LOD**) within Crown's operational environment are the employees who deal directly with Casino patrons or observe patrons at the time of gaming. Within Crown, the business units which form the first line of defence include:

(a) Cage and Count.

(b) Table Games (dealers/croupiers and supervisors).

(c) Gaming Machines (attendants and supervisors).

(d) Surveillance.

(e) Security.

(f) VIP Gaming.

10.2.2 Under a modern risk management regime and under the structure envisaged under the FCCCP, these business units "own" the risks which arise from their operations and, accordingly they are responsible to defend the business from those risks in the first instance.

10.2.3 The employees in these business units are involved in exchanging cash for other value instruments (chips, TITOs etc.), completing threshold reports for exchanges over $10,000, verifying patron identities (KYC processes), observing patron gaming behaviour (both non-verbal and gaming patterns) and observing and tracking patron activity within the Casino.

10.2.4 The information and reporting provided by first line of defence employees enables the AML and Compliance and Surveillance teams to undertake investigations into patron behaviour, assess risks, comply with reporting obligation to AUSTRAC and develop further processes and procedures to mitigate this behaviour.

10.3 Integrity and capability within First Line of defence

10.3.1 For the first LOD to be effective, it is critical the Casino employs low risk individuals and provides quality training which will enable employees to understand their role in AML, the processes and rules which combine to create a strong control environment, how they work and why they are important.

Recruitment

10.3.2 The following summarises the processes by which Crown screens prospective employees. We have focussed on employees who are involved in delivering designated services and are required to hold a Casino Special Employee Licence (**CSEL**) under the Casino Control Act.

[121] We have used pre-COVID as a proxy for the period before the Bergin Inquiry and when Crown was operating with international clientele including junkets

10.3.3 Individuals being considered for a position at Crown providing designated services are subject to due diligence procedures by both Crown and the VCGLR. This involves face-to-face interviews, applicable capability testing, reference checks, police checks, credit assessment and international police checks if the individual has lived outside of Australia in the past 10 years.[122]

10.3.4 Once Crown has satisfied itself as to aptitude for the position and that the candidate is of low risk of corruption or non-compliance with Crown's Code of Conduct and likely to be approved by the VCGLR for a CSEL, an offer will be made to the candidate and Crown will arrange for the CSEL application the VCGLR.

10.3.5 The VCGLR reviews the application, makes its own enquiries and determines whether to issue the CSEL. No person can work at Crown until the CSEL is obtained.

Ongoing employee diligence

10.3.6 Ongoing employee due diligence is undertaken by the AML Compliance team. This includes screening employees using Dow Jones[123] on a daily basis screening employees for exposure to financial crime matters, corruption, drug trafficking, fraud, tax evasion, inappropriate associations etc. Any hits are investigated. Reports are rare and to date all have proved to be false positives.

10.3.7 Crown employees are at risk of being coerced to collaborate with criminals or collude with friends/family/associates in order to de-fraud the casino or conduct other illegal activities such as money laundering.

10.3.8 Crown's surveillance analysts search for signs of potential corruption or collusion by, inter alia,

(a) analysing employee information against patron or other person of interest information (e.g. emergency contacts, addresses)

(b) conducting social media scraping; and

(c) reviewing patterns of play which may connect certain croupiers with certain patrons.

10.3.9 Crown supports its employee through the provision of a whistleblower hotline and an employee counselling service.

10.4 AML/CTF training and awareness

10.4.1 Effective training which covers awareness of money laundering, the typologies and the policies, processes and procedures used by Crown to deter, detect and report is fundamental to giving OTF employees the capability to be an effective first line of defence.

10.4.2 In his FCCCP, Mr Blackburn reports that training has been bolstered in the last 18 months and going forward "*to further advance the effectiveness of our training the FCCP will place a greater focus on financial crime outcomes by tying Crown's efforts in detecting and reporting financial crime to protecting those most vulnerable in our society*".

Survey responses in relation to training issues

10.4.3 In section 12 we provide the details of surveys that we conducted to gather information from Crown employee in regard to matters relevant to AML/CTF, including awareness and training. In this section we have included the responses of OTF employees in relation to their views on their training.

10.4.4 Question: *'How often have you had training in AML/CTF matters?'*[124]

(a) Response: 63% of respondents indicated they receive AML training annually.

10.4.5 Question: *'How would you rate the quality and quantity of the AML training provided to you by Crown?'*

(a) Response:

---

[122] Interview with [redacted]

[123] Third party specialist provider of screening services including of adverse media, credit data, politically exposed persons

[124] OTF Survey: Section 3.4

(b) 75% of respondents indicated the quality and quantity or training provided to them as good or excellent.[125]

(c) The business unit which rated the training at the lowest level was Table Games: 24% of Table Games respondents indicated that the AML training they received is average or poor.

10.4.6 Survey respondents were asked to indicate the format of the last AML/CTF training provided to them. 64% of respondents indicated the last training they received was e-Learning with a test of knowledge; this was followed by 16% of employees indicating they received face to face training lasting less than 30 minutes.

10.4.7 The following comments are from OTF employees in response to an invitation to provide a free test response in relation to the AML training received and their knowledge of money laundering indicators.

No supervision, training can be easily passed by rapidly clicking 'next' without paying attention. This was encouraged by staff to save time

The test is multi-choice and you just keep repeating it until you pass

The AML training offered by Crown just covers the basics. My knowledge of money laundering comes from my own research rather the training offered by Crown.

In person training would be better and absorbed more easily.

Rely too much on e-learning. Same old program year after year.

We are given this training with many other information sessions and it is not given any importance

I feel although I'm taught the signs and indicators of money laundering, it is difficult to determine whether it's money laundering or they just have a lot of money. I feel like these people who money launders are smarter and have more experience than to do these simple signs that we're taught in training.

What I consider suspicious, if my manager does not, the matter goes no further. For instance, I saw a man split up very large amounts of cash between 3 people on the Gaming floor. I considered this suspicious but my manager didn't and that was the end of the matter...

Focus Group comments regarding training

10.4.8 Section 13 includes the output from focus groups conducted involving a range of Crown OTF employees. The Group was asked to comment on the training provided both before and after COVID-19. A summary of their responses and some verbatim comments are included in Table 15.

10.4.9 It is our observation from the discussion that in addition to any formal training (face to face or by eLearning), the OTF employees are involved in considerable levels of on-the-job training.

10.4.10 We observe that the team based, yet highly structured, hierarchical manner in which the floor operates, with layers of responsibility from dealers to pit supervisors to Assistant Casino Managers (**ACMs**) (contributes to on the job learning. Each level within the team has frequent requirements to involve or consult with the next level which lends itself to sharing of information and knowledge.

10.4.11 In addition, from the discussions in the focus groups it appears that the frequent changes to policy and process over the last nine months in addition to the changeable conditions due to COVID-19, has meant that more is conveyed in regular team meetings or pre-shift "musters" during which employees are briefed and reminded of the changes. Employee indicated to us that ML is raised at almost all such sessions.

[125] OTF Survey: Section 3.5

Table 15 Focus Group comments in relation to training

Before COVID-19	Now
▪ AML training is delivered on induction for all departments (runs for around 10 minutes) and then periodically. ▪ 'Crown Learn' (online training created by Crown) is completed annually where staff members have to pass a knowledge check test at the conclusion of the module. If the staff member does not successfully complete the knowledge check at the end of the online course, they are required to keep trying until they pass (there is no remedial training option). ▪ Participants from the EGM[126] division indicated that they receive briefings before their shift a few times a year where they would receive reminders to look out for certain behaviours. ▪ More face-to-face training was held pre-COVID-19 (face-to-face training has been reduced due to the COVID-19 response).	▪ AML training is delivered face-to-face on induction for all departments (runs for around 10 minutes) and then periodically (as for previous state). ▪ During induction, staff are shown a short video provided by AUSTRAC that explains ML, and also go through common ML typologies that run through a casino – they will try to align the AML training with their role. ▪ Crown Learn (online training created by Crown) is completed annually where staff members have to pass a knowledge check test at the conclusion (as for previous state). ▪ Face-to-face training has been held post-lockdown (operations manager presenting to gaming machines staff). ▪ Managers currently undertake a full training day. ▪ Standard Operating Procedures were re-written (and include AML specific sections) and are being rolled-out to all departments. ▪ Some participants indicated that the same amount of AML training has been conducted recently as compared to previously, and that they haven't had face-to-face training since COVID-19. ▪ Some participants indicated that they complete quite a bit of online training. ▪ The surveillance team undertakes comprehensive training to understand their reporting obligations. ▪ Electronic Gaming Machine department participants indicated that they now have briefings at the beginning of every shift where they receive reminders to look out for certain behaviours.
Comments from focus group *"I think we still have the exact same amount of training..."* *"Everyone's fully aware of anti-money laundering, what our responsibilities are and what to look out for."* *"We probably get an overarching...bigger training session because we oversee other areas and we have a lot of responsibility in our space as well...we do a bit more an involved training just for people to understand what our reporting obligations are and if we don't save footage for a particular incident and then 3 months down the track that footage has since expired and then people are looking for it, we're accountable."* (Surveillance team member)	
McGrathNicol observation: – While some employees indicated that they are still receiving the same amount of training as they did prior to COVID-19, the general consensus was that the amount of AML training has increased and there has been a heavier focus on AML since the Bergin Inquiry. – It was noted that the AML team have been running AML training specific to different business units, including how to use the new AML Portal to raise UARs. – It was also noted that the amount of face-to-face training decreased due to COVID-19 restrictions.	

[126] EGM – Electronic Gaming Machine

11 On the floor ML typologies and control framework

11.1 Review of ML typologies and Crown's vulnerability

11.1.1 Crown commissioned a review by Promontory into its vulnerability to recognised ML typologies. Promontory completed its final report on 24 May 2021.[127] Crown has included within the FCCCP a range of proposed additional controls to address the vulnerabilities identified, noting that some controls have already been implemented between Promontory doing its fieldwork and the reporting date.

11.1.2 In Appendix C we have summarised in a table the vulnerabilities faced by Crown and noted the controls in place as identified by Promontory and information gathered by us in the course of our work including review of policies, procedures and rules as well as interview and focus groups.

11.1.3 The residual weaknesses for each vulnerability, which indicates the need for additional controls, are set out in Table 16 together with the controls which Crown proposes to implement according to pages 37 to 41 of the FCCCP paper presented to the Board[128] on 24 May 2021.

11.1.4 In regard to the proposed timing, we refer to our general comments regarding the dependencies of the FCCCP, in particular in regard to technology upon which the introduction of some of the proposed controls rely.

11.1.5 McGrathNicol has utilised money laundering typologies as identified within Financial Action Task Forces (FATF) report 'Vulnerabilities of Casinos and Gaming Sector 2009' within our review of Crown's control weaknesses and control as identified by Promontory in their Vulnerability Assessment.

[127] CRW.512.086.003

[128] CRW.512.081.1786

Table 16

Typology & Current Weakness	Crown Proposed Controls & Timing[129]	McGrathNicol comment
[redacted]		

[129] CRW.512.112.0034: Annexure B: Crown's Response to Recommendations and Findings in Promontory Vulnerability Assessment dated 24 May 2021 and FCCCP CRW.512.081.1788 p 37-41

Typology & Current Weakness	Crown Proposed Controls & Timing[129]	McGrathNicol comment
[redacted]	[redacted]	
Utilising Safety Deposit Boxes SDB's used to park funds or items illegally gained or storing for a third party to collect.	▪ Return property in safety boxes to patrons. – Aim to return all property to patrons as soon as possible.	▪ Risk will be fully mitigated once all property has been returned to the appropriate patrons.
[redacted]		

Typology & Current Weakness	Crown Proposed Controls & Timing[129]	McGrathNicol comment
[redacted]		

Typology & Current Weakness	Crown Proposed Controls & Timing[129]	McGrathNicol comment
[redacted]		

12 Surveys of Crown employees

12.1 Purpose

12.1.1 The capability, awareness, knowledge and attitude of the people in the first and second lines of defence are critical to the success of an organisations AML/CTF program. In order to capture the views of a greater number Crown employees, we undertook two independent surveys of a sample of employees in each of the following categories:

(a) For Survey 1 - Employees in the first line of defence who hold a Casino Special Employee Licence (**CSEL**);[130]

(b) For Survey 2- Employees in roles related to the second line of defence from AML, legal, internal audit, compliance, regulatory and risk assurance. In this regard we note that these employees are not necessarily AML focussed as at the time, the AML second line of defence had not been developed into the structure now proposed under the FCCCP.

12.1.2 The objective of the surveys was to gain an understanding employees' direct experience of money laundering activity at the Casino, their understanding of AML controls and processes, the training they have received and the culture as it pertains to tolerance of money laundering and AML compliance.

12.1.3 The surveys also provided Crown employees an opportunity to provide other information about their experience at Crown in regard to AML/CTF which they wished to share.

12.2 Methodology

12.2.1 The survey questions were created by McGrathNicol and loaded into Qualtrics, a cloud-based provider of survey software. The survey was issued by the provision of a link to a secure internet site to a sample of Crown Melbourne employees.

12.2.2 To establish the sample, Crown provided McGrathNicol with a listing of Crown Melbourne employees in each category together with the business unit in which they work and the hours worked during 2020 and 2021.

12.2.3 From the listing provided by Crown, McGrathNicol:

(a) Excluded any employees who had not worked hours in 2021;

(b) Excluded employees in business units which we considered would have little exposure to the activities relevant to AML/CTF, including Marketing, Human Resources, Hotel Operations and Entertainment;

(c) Identified the remaining number of employees within each business unit to be surveyed;

(d) Determined the size of the sample for each business unit; and

(e) Selected the employees to be surveyed.

12.2.4 The survey was distributed on 25 May 2021. McGrathNicol sent the survey link to employees who had Crown email addresses and Crown sent the survey link to the private email or text numbers for those employees who did not have Crown addresses (approximately 60%).

12.2.5 Crown issued the survey under a statement from the CEO encouraging employee participation and ensuring employees of anonymity. Employees were offered a range of ways to complete the survey including at Crown's offices or McGrathNicol's offices. A reminder email was sent to employees 3 days after it was issued.

[130] An CSEL is a license issued by the VCGLR pursuant to the Casino Control Act 1991 and which must be held by anyone who has a role in the casino managerial or decision making capacity with respect to casino operations and all those who are involved in conduct of gaming; handling of cash; handling of chips; security and surveillance; gaming machine operation, repair or maintenance; supervision of these activities and any other activities as specified by the VCGLR.

12.2.6 The survey was initially open for 1 week, but after the Casino went into COVID-19 lockdown on 28 May 2021 the surveys were extended for a further week to 8 June 2020 by a notification which included a further message of encouragement to complete the survey.

12.2.7 Table 17 summarises the population and sample sizes for each survey as well as the number of respondents to each survey. The response rates are sufficient to give the results of the survey a confidence level in excess of 90% such that the results may be interpreted as representative of the relevant population.[131]

Table 17

Survey profiles							
Survey		**Population**	**Sample**	**Sample as % population**	**Respondents**	**Respondents as % of sample**	**Respondents as % of population**
1	Casino Special Licence holders						
	Cage and count	122	122	*100%*			
	Gaming machines	262	150	*57%*			
	Security & services	205	35	*17%*			
	Surveillance	71	71	*100%*			
	Table games	2,237	1,000	*45%*			
	VIP gaming	22	22	*100%*			
		2,919	**1,400**	***48%***	**342**	***24%***	***12%***
2	Other relevant employees						
	Finance	3	3	*100%*			
	Crown Limited	1	1	*100%*			
	Legal	6	6	*100%*			
	Legal & regulatory	38	38	*100%*			
		48	**48**	***100%***	**39**	***81%***	***81%***
Total		**2,967**	**1,448**	***49%***	**381**	***26%***	***13%***

12.3 Survey questions

12.3.1 The questions posed in the survey included multiple choice seeking a single response, multiple choice where all that applied could be selected and free text. The majority of questions allowed for free text to be added to explain the answer given.

12.3.2 In several areas, the questions were designed to derive an understanding of employee's perception of changes in the AML/CTF landscape. For this purpose, we used the terms "before COVID-19" and "now" so as to take employees attention to times before the disruptions of COVID-19 and before the ILGA Inquiry was advanced. This places "before" as being earlier than February/March 2019.

12.4 Survey results

12.4.1 The detail of the results for survey 1 – CSL holders is in Appendix E

12.4.2 The detail of the results of survey 2- Second line of defence employees in Appendix F

12.4.3 The sections which follow provide the key findings from the surveys.

12.5 Survey findings – Experience of money laundering at Melbourne Casino

12.5.1 Within the surveys, respondents were asked a range of questions surrounding whether they believed money laundering has occurred or is still occurring within Crown Casino.

[131] Determined by use of the using the sample size calculator from the website of the Australian Bureau of Statistics https://www.abs.gov.au/webs tedbs/d3310114.nsf/home/sample+size+calculator. *342 responses in survey 1 are sufficient to result in a 95% degree of confidence that the results are representative of the population; 39 responses in Survey 2 are sufficient to results in a 92.5% degree of confidence.*

12.5.2 Employees were asked *'thinking back to the times before COVID-19, in your opinion, how likely is it that money laundering activities were then being undertaken at Crown?'*

(a) The following results were noted within the OTF survey:[132]

(i) 72% of respondents indicated that they believe it is likely that money laundering was occurring at Crown prior to COVID-19.

(ii) Breaking the responses down by business unit it was noted that 100% of surveillance respondents believe money laundering was likely or extremely likely to have occurred prior to COVID-19 whilst 70% of VIP Gaming staff and 70% of Table Games staff believed money laundering was likely to have occurred prior to COVID-19.

(iii) Breaking the responses down by employment tenure at Crown; 77% of employees who have worked at Crown for 5 or more years believe that it is likely that money laundering was occurring prior to COVID-19, whilst only 45% of employees who have worked at Crown between one and three years believe it is likely that money laundering was occurring at Crown prior to COVID-19.

(b) The following results were noted within the second line of defence survey:[133]

(i) 81% of survey respondents indicated they believe it is likely or above that money laundering was occurring at Crown prior to COVID-19. Breaking the results down by department, 100% of the AML business unit indicated that it is likely or above that money laundering was occurring at Crown prior to COVID-19.

12.5.3 Employees were also asked to indicate whether *'at the current time, how likely is it that money laundering is occurring at Crown Melbourne?'*

(a) The following results were noted within the OTF survey:[134]

(i) In this instance, 50% of OTF employees indicated that they believed it was either unlikely or very unlikely that money laundering was currently occurring at Crown.

(ii) Notably, 85**%** of surveillance staff indicated that they believe money laundering is currently occurring at Crown. This was in contrast to 67% of VIP Gaming staff who responded that that it is unlikely that money laundering is occurring at the current time.

(iii) We suggest these contradictory responses are due to the cessation of junkets and minimal international patrons due to COVID-19 travel bans. Further, it may be that Surveillance have a stricter sense of what money laundering is and include small-time money laundering from black economy small business whilst the VIP team think of it as connected to organised crime.

(b) The following results were noted within the second line of defence survey:[135]

(i) 43% of second line survey respondents indicated it they believe it is either unlikely or extremely unlikely that money laundering is occurring at Crown currently.

(ii) Notably 100% of the AML business unit still believe that money laundering is likely, highly likely, or extremely likely to be occurring at Crown currently.

(c) The following sample of free text commentary was provided by second line of defence survey respondents in relation to their opinion on whether money laundering is currently occurring at Crown:

It is impossible to completely eliminate the risk that customers are dealing with the proceeds of crime while participating in gaming activity at any casino, just as it would be for traditional banking customers interacting with the financial system. However, Crown is hardening the environment against these risks through additional controls and monitoring, to reduce the impact and scale of these risks.

As a Casino operator, Crown is susceptible to Money laundering. Casinos are a common vehicle across the world for criminals to clean their money and casinos have controls in place to mitigate that risks.

---

[132] OTF Survey: Section 2.3

[133] Second Line Survey: Section 2.4

[134] OTF Survey: Section 2.2

[135] Second Line Survey: Section 2.3

The Casino is vulnerable to ML. You cannot eliminate it however you can disrupt and deter such activity through identification and mitigation. In fairness to the casino sector, it's my view that no one in the financial sector such as banks could say ML is not occurring in their business.

12.5.4 Survey respondents were also asked to answer questions regarding their personal experiences at the Casino regarding money laundering or suspicious behaviour. Employees were asked to respond to the following question with either 'Yes' or 'No' response. *'I have personally witnessed behaviour that was suspicious and may have been indicative of money laundering at Crown Melbourne'.*

(a) On-the-floor survey respondents provided following responses:[136]

(i) Overall, 53% of respondents indicated that they have not personally witnessed behaviour that may have been indicative of money laundering.

(ii) By business unit, 67% of Cage and Count staff and 69% of Surveillance staff indicated that they have personally witnessed behaviour that may have been indicative of money laundering.

(iii) 54% of staff who have worked at Crown for over 5 years indicated they have witnessed behaviour indicative of money laundering whilst 79% of staff who have worked at Crown between one and three years indicated that they have not witnessed behaviour, which may have been indicative of money laundering.

(b) Second line of defence survey responses provided the following responses:[137]

(i) 72% of respondents indicated they had not personally witnessed suspicious behaviour that may have been indicative of money laundering and 20% indicated that they had witnessed such behaviour prior to February 2021.

12.5.5 Employees who answered 'Yes' to witnessing behaviour indicative of money laundering were asked to provide a comment of examples of the incidents they noticed.

(a) Below is a sample of on-the-floor survey comments:

Threshold transactions, Suspicious transactions just below the threshold, Large non-threshold transactions with little or no play

I have observed just about every type of suspect transaction possible; structuring to avoid having to provide ID, large transactions not commensurate with rated play, loan sharking, unknown sources of chips and cash. They are usually reported by 3rd parties and investigated by my team.

Bill stuffing remote gaming terminals, Patrons presenting significant value of cash chips at the Cage without corresponding gaming ratings, Patrons exchanging chips between each other, Large cash buy-ins with no rated gaming

(b) Below is a sample of second line of defence survey comments:

Unexplained source of wealth; sending program winnings to a third party; large cash buy-ins; bags of cash

Given my role in the AML space I see activities through transaction monitoring of behaviour that is suspicious, This includes structuring of transactions, gaming trends (changes to gaming patterns, increase in average bet, losses), gaming which is inconsistent with the customers known source of wealth, cash transactions which are inconsistent with historic gaming patterns, transactions not supported by gaming activity, transactions on a customers account which is inconsistent with gaming activities etc.

Potential attempted structuring behaviour

People buying in for multiple amounts below 10k in order to avoid a threshold transaction.

Individuals cashing in large amounts on TG and not playing - going straight to the cashier. Cashing 10k and then removing some when asked for ID.

[136] OTF Survey: Section 5.6

[137] Second Line Survey: Section 2.6

12.5.6 On-the-floor employees who noted that have witnessed behaviour indicative of money laundering not being reported made the following comments as to why these may not have been reported:

> *Too much hassle for Area Managers and not enough support from their superiors, who have an interest in permitting that behaviour*
>
> *Reporting is done by frontline workers as is required. Those reports have then been ignored at higher levels.*
>
> *The manager or managers think is not necessary because under $10k payout.*
>
> *Suspicious behaviour prior to January 2021 was not reported. Since the training in January of this year, suspicious behaviour seems to be reported.*

12.6 Survey findings – AML/CTF training and awareness

12.6.1 Survey respondents were asked a range of questions surrounding the type of AML training they receive at Crown, the frequency of this training, the quality of the training and questions aimed to understand staff's confidence in their knowledge about a range of money laundering issues.

12.6.2 OTF employees were asked *'how often have you had training in AML/CTF matters?'*[138]

(a) 63% of respondents indicated they receive AML training annually.

12.6.3 Second line of defence employees were asked *'how often have you had training in AML/CTF matters?'*[139]

(a) 42% of responses indicated they receive AML training annually.

12.6.4 Employees were asked *'how would you rate the quality and quantity of the AML training provided to you by Crown?'* Respondents could answer either excellent, good, average, poor or other.

(a) OTF survey employees indicated the following:[140]

(i) 75% of respondents indicated the quality and quantity or training provided to them as good or excellent.

(ii) The business unit which rated the training at the lowest level was Table Games. 24% of Table Games respondents indicated that the AML training they received is average or poor.

(iii) 26% of employees who have worked at Crown for over five years indicated the AML training they receive is average, poor or other. This is compared to employees who have worked at Crown between one and three years; 21% of employees indicated the training was average and 0% indicated the training was poor.

(b) Second line of defence survey employees indicated the following:[141]

(i) 92% of survey respondents indicated the training they received was either good or excellent.

(ii) The difference in responses between the OTF and second line population suggest an ongoing challenge in maintaining knowledge and awareness within the first line of defence.

12.6.5 Survey respondents were asked to indicate the format of the last AML/CTF training provided to them.

(a) 64% of respondents indicated the last training they received was e-Learning with a test of knowledge; this was followed by 16% of employees indicating they received face to face training lasting less than 30 minutes.

12.6.6 Survey respondents were provided the opportunity to add commentary surrounding the AML training received and knowledge of money laundering indicators. Below is a sample of comments provided by OTF employees:

---

[138] OTF Survey: Section 3.4

[139] Second Line Survey: Section 3.4

[140] OTF Survey: Section 3.5

[141] Second Line Survey: Section 3.5

No supervision, training can be easily passed by rapidly clicking 'next' without paying attention. This was encouraged by staff to save time

The test is multi-choice and you just keep repeating it until you pass

The AML training offered by Crown just covers the basics. My knowledge of money laundering comes from my own research rather the training offered by Crown.

In person training would be better and absorbed more easily.

Rely too much on e-learning. Same old program year after year.

We are given this training with many other information sessions and it is not given any importance

I feel although I'm taught the signs and indicators of money laundering, it is difficult to determine whether it's money laundering or they just have a lot of money. I feel like these people who money launders are smarter and have more experience than to do these simple signs that we're taught in training.

What I consider suspicious, if my manager does not, the matter goes no further. For instance, I saw a man split up very large amounts of cash between 3 people on the Gaming floor. I considered this suspicious but my manager didn't and that was the end of the matter

12.6.7 The survey results combined with the comments provided indicate an emphasis of quantity over quality of training.

12.7 Survey findings – Culture and resources

12.7.1 Within the survey provided to Crown employees a number of questions were asked regarding Crown's culture in relation to money laundering, management support regarding detection and reporting, staff encouragement to report, pressures that face staff from customers or management and staff observations of Crown's culture.

12.7.2 Staff were asked to indicate whether they *'are encouraged to report any unusual or suspicious behaviour or transactions which may indicate money laundering'.* Respondents were given the ability to select answers ranging from Strongly Agree to Strongly Disagree.

(a) A sample of OTF comments are provided below:[142]

(i) Overall, 87% of OTF employees indicated that they agree or strongly agree that they are encouraged to report suspicious behaviour.

(ii) 100% of Cage and Count, Gaming Machines and Security agreed or strongly agreed with this question.

(iii) Table Games respondents were the only business unit to disagree with this question with 8% of respondents indicating they either disagree or strongly disagree with this question and 13% neither agreeing nor disagreeing with the question.

(b) Second line of defence employees provided the following responses to this survey question:[143]

(i) 92% of respondents indicated they either agreed or strongly agreed regarding being encouraged by managers to report suspicious behaviour with 8% of respondents indicating they neither agree nor disagree.

12.7.3 Survey respondents were asked about Crowns treatment of VIP Customers. Specifically, respondents were asked to agree or disagree with the following statement: *'VIP customers are treated just the same as the non-VIP customers when it comes to how they are observed and reported at the Casino.'*[144]

[142] OTF Survey: Section 4.1

[143] Second Line Survey: Section 4.1

[144] OTF Survey: Section 5.3

(a) 39% of respondents either agreed or strongly agreed that VIP customers were treated the same as non-VIP customers, whereas 61% of respondents either disagreed, strongly disagreed or neither agreed nor disagreed.

(b) 62% of surveillance respondents and 55% of security respondents indicated they either disagreed or strongly disagreed that VIP customers are treated the same as non-VIP customers when it comes to observation and reporting.

(c) Respondents were given the opportunity to provide an explanation or comment on their answer to this question. Below are a sample of free text comments provided by OTF survey respondents:

Absolutely not, VIP players are allowed to become intoxicated, assault staff, have sex in toilets, verbally abuse staff, spit at (or near) staff, and do dodgy transactions as a matter of routine in VIP areas.

They pretty much have the run of the place, for instance I once had a VIP patron claim a losing bet was a colour change and her money was refunded, that wouldn't happen on the main floor

VIPs are treated differently, they are VIPs.

VIP customers are frequently treated in a preferential manner to non-VIP customers

Vip customers get a completely different treatment momey talks

They get better treatment and dealers to there liking

VIP customers are given whatever they want whenever they want. Crown probably dont want to keep VIP's waiting so corners do get cut.

They are allowed special privileges. We are asked to bend SOP s when dealing with high values customers..

There is a very clear distinction between VVIP customers and main Gaming floor customers. My understanding of VVIP is there is greater leniency with those customers and what they are able to do.

Please ... it's a Casino. They are what pays the bills so they are given more rein

In the past I would answer this question as Disagree as there were things that VIP customers did that were not reported. But now with the changes made / focus on compliance and reporting there is no differentiation. In fact I believe that the VIP customers will now come under more scrutiny and subjected to more reporting than a non- VIP.

12.7.4 The free text responses provided to this question indicate that VIP and VVIP have been afforded leniency, although one respondent was of the view that this had changed and such leniency will not continue. This suggest that Crown faces a significant challenge in re-calibrating employee's understanding of what will and won't be tolerated.

12.8 Survey findings – Changes in AML/CTF controls and focus

12.8.1 Within the second line of defence survey respondents were asked whether *'they believe that Crown takes its role in detecting and reporting AML/CTF activity very seriously'.*[145]

(a) Overall, 67% of respondents indicated that '*Yes Crown always has'* and 33% of respondents indicated that '*Yes it [Crown] does now'.*

(b) Notably within the AML business unit 57% of respondents answered '*Yes – it does now*'.

(c) A sample of comments free text comments made by the second line provided below. Free text commentary surrounding the above question included the following:

The importance of AML/CTF has been steadily increasing over the past 3-4 years

I have noticed an uplift since appox. 2017

[145] Second Line Survey: Section 5.9

Based on my visibility of the culture I believe the detecting and reporting was always taken seriously however prior to ILGA and the associated adverse media there was little awareness of what constituted a strong AML compliance action.

12.8.2 Overall the responses indicate a current view that Crown presently takes its role in detecting and reporting ML/TF activity very seriously, two thirds of respondents of the view that this has always been with the balance of the view that getting to this state has been a more recent development although those that date the change place it back to before the Bergin Inquiry.

12.8.3 Within the second line of defence survey respondents were asked about the capability and diligence of the first line of defence over the past 3 months as compared to the period prior to COVID-19.[146]

(a) Overall, 67% of respondents indicated they believe the capability and diligence has improved substantially.

(b) Notably, 100% of AML business unit respondents believe the first line of defence capability and diligence has improved substantially.

12.8.4 Survey respondents were asked to provide commentary regarding:

(a) the level of activity at Crown pre and post COVID-19 including indications of money laundering or suspicious behaviour;

(b) what more Crown could be doing to deter, detect or report money laundering; and

(c) any other comments they would wish to convey to the commission in relation to financial crime at Crown.

12.8.5 A sample of comments made by the second line survey respondents is provided below:

The difference is night and day. Previously we were very good at reporting, but rarely investigated the source of funds. We have since created whole teams of industry experts who's only job is to investigate our patrons source of wealth/funds.

Staff & management are trained to be more alert

It seems that international "VVIP" players are the epicentre of money laundering. As this has been severely curtailed by the pandemic it seems to have slowed down.

There have been many changes made in regards to sending money to Crown bank accounts that have made "potential" laundering much more difficult if that is our patron's intentions.

This also applies to cash presented at Crown.

Both of these changes have made it much less likely that laundering is occurring.

staff (particularly in Table Games) have been much more proactive in reporting suspicious activity. It's hard to tell if the volume of suspicious activity is higher or just how often it's being reported

There is a lot more reporting now. Staff are also reporting on a larger variety of indicators. It is clearly becoming a greater focus across the business.

Crown has been very vigilant since coming back post covid and are very determined to keep the Casino clean and free of money laundering to the best of their abilities.

12.8.6 In regard to what more could be done to improve detection, deterrence and reporting of ML a sample of comments from OTF and second line respondents is provided in Table 1Table 18 below:

[146] Second Line Survey: Section 5.4

Table 18

OTF[147]	Second line of defence[148]
▪ *I believe we are doing very well now on this issue. The increased focus and process changes including KYC. The requirement for SOF forms to be completed once $25k cash has been presented by a customer in a day. All brings more scrutiny on the financial transaction. Going cashless would be my only suggestion of improvement.* ▪ *More regulation within the frame work of the loyalty program. Regulation in the use of unsupervised automatic table games. More presence of vcglr staff on the Gaming floor including VIP areas* ▪ *Increased staffing levels for the AML and Surveillance teams.* ▪ *Going to a cashless system of gambling could all but eliminate money laundering. But that would be a major adjustment.* ▪ *A training day aimed at all staff that is in person with a qualified staff member who is confident.* ▪ *Teaching by government (not e-learning) employees on this subject.* ▪ *Crown should change their culture so they aren't so desperate for money. It's kind of embarrassing really. Simply stop being so money hungry and raise the standards.* ▪ *Only accept bank transfers or have a tap an go system so we know all the money is coming from financial institutions.* ▪ *Only accept bank transfers or have a tap an go system so we know all the money is coming from financial institutions.* ▪ *all players could be required to have carded play, that way money swapped for chips on tables or inserted to EGM's can be recorded as they move around and get unnoticed* ▪ *Working together with AUSTRAC and Law enforcement.*	▪ *They could link each of the separate systems to each other. That way we would have a better picture of who we are investigating, and what out comes are achieved. Also by identifying PEP's and adverse media before allowing new customers to join Crown.* ▪ *Projects to improve systems and people capability are already underway and are critical to providing increased insight and effectiveness to AML investigations* ▪ *continue to provide updated and enhanced training, share more examples of activity which has been noticed and reported, continue to be vigilant* ▪ *Photos printed on Rewards Cards. Set lower thresholds for requiring a customer to join and present a membership card for the purpose of tracking their gaming activity and transactions.* ▪ *Crown should continue on its work and not become complacent and reinforce training with employees particularly the front line of defence employees and the gaming sales and host employees* ▪

Source: McGrathNicol surveys

12.8.7 In relation to any other comments they would wish to convey to the commission in relation to financial crime at Crown, a sample of comments from OTF and second line respondents is provided in Table 1Table 19 below:

[147] OTF Survey: Section 5.15

[148] Second Line Survey: Section 5.12

Table 19

OTF[149]	Second line of defence[150]
▪ *You need outside people undercover that have the responsibility of looking for illegal activity on the Casino Floor. Hoping that 'Crown' Staff will report it is a fantasy* ▪ *All players in Pit 8, Maple Room should be carded. Too many patrons playing uncarded and funds can't be tracked. Patrons not being tracked for their buy ins, however then cash out large amounts of chips at the Cages which can't be verified by their ratings.* ▪ *In my time at Crown, I can list many many times where things have been either covered up, not reported to the VCGLR as required, or a blatant disregard for the law/casino control act have occurred. Long serving Middle Management is the issue, not the recent board members that resigned. They think they are above the law, and make decisions that are not in-line with Crown's policies or their requirements under the law.* ▪ *Crown is a sewer, the workplace culture is toxic and the company profits the more money comes in. Players are allowed to get away with murder so long as they keep playing. Crown's attitude toward the law and regulation is to be seen to do enough to keep the heat off, while continuing to push the envelope. Crown cannot be trusted to abide by the law, any serious investigation will prove damning. I encourage the commission to delve deep and not let Crown get off scot free* ▪ *It is a very different world and culture here now than it was two years ago.* ▪ *The key issues raised over the last few years have related to junkets and other casino groups operating within Crown (Sun City, for example). These have had sweeping changes, where Crown no longer associates with these groups. Additional check are now performed on VIP patrons with much more scrutiny overall.* ▪ *While I believe that ML issues can never be entirely eliminated from the Casino, Crown is trying to address as many issues as it can.* ▪ *Prior to January 2021 Crown had a no questions asked approach to customers bringing money into the Casino. e.g. the amount brought in, amount gambled away, was the patrons private business. Staff were not encouraged to question or report suspicious behaviour. VIP's were treated in this way to a greater degree than the general public.*	▪ *While my tenure at Crown, I have really seen a more enhanced and detailed attention to tackling financial crime. Furthermore, there has been a significant shift in culture for the better and there is really been a push to do the right thing. Not commenting on the past processes given I was not working at Crown at the time, I do really believe Crown has opened up to feedback and is working hard, efficiently and quickly to enhance its processes around compliance and combatting AML.* ▪ *My time at Crown has demonstrated to me that as an organization, Crown has continued to train staff on AML/CTF matters, and other relevant training. Crown has enforced a culture of compliance and integrity since I commenced working for Crown.* ▪ *I'm privileged to be part of a team involved in the uplift of compliance relating to AML. My view is that Crown is already exceeding the minimum standards required by legislation, and within the next 6-12 months, Crown will have the strongest and most effective AML regime of any Casino in Australia (confident it already does).* ▪ *Many bad decisions were made by those in higher management (who are no longer with us) and I feel a lot of their decisions were directly linked to their bonuses and remuneration.* ▪ *Crown's past is behind it and it is a new Crown and focus should be on the future not past matters which may have occurred over 4, 5 to 10 years ago.* ▪ *The steps Crown has taken in the last 24 months to identify, manage and mitigate ML/TF risk are ahead of what the broader industry is doing. What started under its previous management and continues to do today will be world leading, beyond industry standards and will far exceed regulatory requirements. I think the Commission would benefit to understand what other casinos in the Asia Pacific Region are doing in relation to identifying, managing and mitigating ML/TF risks both now and before the issues with Crown were identified to get an understanding of what the industry standards are (and were pre mid 2019).*

Source: McGrathNicol surveys

12.8.8 McGrathNicol makes the following observations in relation to the survey results obtained from both the OTF employees and second line of defence employees:

(a) Consensus amongst most survey respondents was that money laundering cannot be completely eliminated within the casino, but the newly implemented controls and planned controls will detect more of this behaviour.

[149] OTF Survey: Section 5.16

[150] Second Line Survey: Section 5.13

(b) Employees noted a significant shift in culture and emphasis on AML/CTF over the past 4 years and Crown are now actively implementing processes, procedures, policies, improving training, implementing technology solutions and increasing resources in order to strengthen their AML program.

(c) Employees agreed they believe money laundering was occurring at Crown prior to COVID-19 and it is less likely to be occurring at the current time.

(d) Majority of employees noted they feel supported and encouraged by managers to report suspicious behaviour which may be indicative of money laundering.

13 Focus Groups

13.1 Purpose

13.1.1 In addition to the surveys addressed in section 12, McGrathNicol facilitated some focus groups in order to gain insight as to how AML/CTF controls and processes operate in reality and to discuss potential money laundering scenarios and how they play out in Melbourne Casino. Focus groups were held with two groups of employees:

(a) OTF – Two focus groups were conducted each with a different group of employees including representatives from Cage, Security, Surveillance, Table Games, EGMs and VIP Services.

(b) Employees from AML, legal, internal audit, compliance, regulatory and risk assurance (**2LD**).

13.1.2 Details of the focus groups are shown in Table 20.

Table 20

Details of Focus Groups				
Group	**No of participants**	**Time held**	**Date held**	**Duration**
OTF - Group 1	7	9.15am	Wednesday, 23 June 2021	3.0 hours
OTF Group 2	8	2.00pm	Wednesday, 23 June 2021	3.0 hours
2LD	9	2.00pm	Thursday, 24 June 2021	2.5 hours

13.2 Methodology

13.2.1 From a list of employees provided by Crown, McGrathNicol identified the roles which it wished to have represented at each of the OTF and 2LD focus groups and identified nine preferred attendees for each focus group. Because participation was voluntary, Crown was provided with a list of acceptable substitutes for each identified participant so that each focus group would have sufficient numbers and would have appropriate representation of roles.

13.2.2 McGrathNicol provided Crown with a draft invitation to potential participants and Crown contacted the employees to seek their involvement. Key aspects of the focus groups were that:

(a) Attendance was voluntary

(b) Participants were assured that any reporting of the focus group would be on basis that did not allow for their identification

(c) Each focus group was recorded sole to assist with accuracy of reporting of what was said

(d) Each focus group was observed by a representative form Allens, acting for Crown

(e) Participants were provided with alternative means of contacting McGrathNicol should they wish to make a contribution on a more confidential basis.

13.2.3 Each focus session involved two parts:

(a) Open discussion prompted by a range of questions concerning Crown operation, environment, culture and AML processes and controls; and

(b) Discussion of a number of prepared scenarios involving common money laundering typologies. Across the two OTF focus groups 11 scenarios were discussed and the 2LD focus group extended 5 of these scenarios by identifying what would have occurred from their perspective.

13.3 Focus group themes and observations

13.3.1 Appendix G comprises reports of the themes covered in the focus groups including:

(a) Observations of Previous State;

(b) Observation of Current State;

(c) McGrathNicol Observations;

(d) Focus Group Observations; and

(e) Illustrative comments made by focus group participants.

13.3.2 Table 21 is a summary of the themes raised within the focus groups and a sample of quotes made by focus group participants.

Table 21

Theme	McGrathNicol Observations	Focus Group Quotes
Money Laundering Awareness (OTF)	▪ It appears that employees have an increased awareness of ML since the Bergin Inquiry due to increased training and communication.	*"Prior to lockdown...prior to the Bergin Report, AML was a thing of course..."*
Potential Money Laundering examples	▪ The focus groups were able to provide ML examples and it appears that they have adequate knowledge of basic methods used to launder money in a casino and what to look out for.	
Suspected an actual ML incident	▪ The focus groups noted a number of suspected ML incidents and it appears that the nature of these incidents has not changed much aside from the fact that there has been a reduced number of patrons since COVID-19.	*"Recently there was an example...a player came in and basically bill stuffed machines across the property over 3 or 4 hours to the value of about $40,000. Every 30 minutes or so he would press collect and the ticketing system...would spit out a ticket from the machine which would then require a cheque to be issued because anything over $2,000 must be paid by cheque. This guy...ended up with something like nine gaming cheques...our department reconciles / issues all the gaming cheques...real standout...one patron across such a small period of time, ranging from values of $2,000 up to $10,000...they can go in and see what actual activity there was on those individual machines...they become unverified cheques...reporting done to our AML team along the lines of a UAR ...potentially the patron will be 'WOLd'."*
AML Awareness Training (frequency and effectiveness)	▪ While some employees indicated that they are still receiving the same amount of training as they did prior to COVID-19, the general consensus was that the amount of AML training has increased and there has been a heavier focus on AML since the Bergin Inquiry.	*"I think we still have the exact same amount of training..."* *"Everyone's fully aware of anti-money laundering, what our responsibilities are and what to look out for."*

Theme	McGrathNicol Observations	Focus Group Quotes
AML Culture (OTF)	▪ It appears that some staff believe that there was nothing wrong with the AML culture because they were always encouraged to report suspicious behaviour. ▪ This was in contrast to other staff who said that there is now increased pressure to report suspected AML activity correctly because they have received so much AML training and their jobs are on the line.	*"Now we've been trained so much and we've had all this training, so our jobs are on the line if something happens, so a 'no' is a very common thing."* *"If we suspect it, we report it...we can't stop it, we're not the police."* *"The culture's good, people are...I don't think any different to the way they were before."* *"Our team completely understand what's involved and why it's needed and why it's so important, we always have."*
AML Culture (other than OTF)	▪ It appears that AML / Compliance staff believe that the culture around AML was always good and will improve due to increased resourcing.	*"Never in the time have I been here, I've never been aware of where we would tell staff not to submit a suspicious matter report if they believed it to be suspicious, however I guess simply you come back now, the increasing numbers, there is no doubt there's been a heavier push, education process...end result of that is that we have significant numbers of SMRs that are submitted."*
Resourcing (AML Team)	▪ It appears that the employees acknowledged that the AML team numbers were inappropriate (in hindsight) and Crown was already starting to increase their AML focus prior to the Bergin Inquiry (particularly once Louise Lane started at Crown), however it appears that the Bergin Inquiry expedited Crown's plans to grow their AML team because it became necessary to keep their licence.	*"Logically...the numbers weren't appropriate, but the company believed they were, obviously, and whether that's dollar-driven or not, it's for others to also answer, but getting resources has not always been a simple answer in most departments."*
AML Team function (effectiveness)	▪ It appears that the AML team has become more effective since the numbers have increased and the Joint AML/CTF Program has been introduced.	*"The programs prior to the Joint Program weren't dissimilar...they were fairly well-aligned."*
Communication of AML Policies and Procedures	▪ It appears that there has been good communication of AML policies and procedures.	
AML Conduct by OTF personnel	▪ It appears that the most significant change for floor staff has been the SOF Policy, which now requires a patron to complete a SOF form for transactions totalling more than $25,000 in a particular day. Previously it was at their discretion and SOW details would only be reported if they had a reason to think that the patron was suspicious.	*"Before, we didn't have limits...we would be keeping an eye on it ourselves and then obviously there would be an investigation when the amount got crazy...but now we have the source of funds..."* *"Players bringing in $150,000...and then they would always get a suspect transaction done on them."* *"Since the Bergin Inquiry we've now gone to having a policy where they must actually declare where the money's from...above a certain threshold...and I would say probably 2 out of every 3 are probably rejected."*

Theme	McGrathNicol Observations	Focus Group Quotes
Observation of improper customer / OTF personnel relationships	▪ It appears that the risks around employees being groomed by patrons have decreased since the new rule that patrons are no longer permitted to request a particular dealer without approval from the ACM.	*"Say...a dealer is friends with a patron... he won't take his losing bets."*
Avenues for reporting AML concerns (OTF personnel)	▪ It appears that there has been an increase in the number of UARs submitted (compared to SMRs previously) due to the new, user-friendly AML Portal and increased AML training and awareness. ▪ All employees were very familiar with the UAR concept and process; most had completed and UAR, although some just report incidents to their manager who inputs the UAR (eg croupiers cannot leave their tables)	*"It's not like it was hard."* *"People had the training."*
AML risk level	▪ It appears that the AML risk level has decreased since the introduction of new AML policies and procedures.	*"It is clear that we've made mistakes ...I'm just saying that we didn't deliberately mean to do those things."* *"With everything they're currently doing, if we're not in a better spot well then we're clearly stupid people."*
Technical functionality	▪ It appears that Crown has extensive surveillance systems which assist the AML team, including a high definition facial recognition system which even has the ability to recognise people wearing disguises. ▪ It also appears that transaction monitoring has become more effective since the introduction of Sentinel.	*"We've got fantastic images at all the entry points and...all the outer points so that we're alerted to people before they actually approach the entries, we've got plenty of time...those photos are obtained from those cameras which are really high definition."*
Know your customer protocols	▪ It appears that the AML team has placed greater pressure on the individual departments to collect information on customers.	*"That's why you have to know your customer...so it's easy to approach them...if you build the relationship it's easy to talk to them."* *"Once you go to silver, or go up a tier, every six months... on the first of October and on the first of April they have to come to Crown to renew the card again."*

13.4 Focus group scenario analysis

13.4.1 During the three focus groups conducted by McGrathNicol, a number of scenarios were presented to the focus group participants. The objective of the focus group scenario discussions were to determine the participants awareness of different money laundering typologies which may occur within a casino, how these types of activities may be detected, what controls are in place to detect or deter this behaviour from happening and what Crown staff would do if this behaviour was noticed including reporting obligations.

13.4.2 Specifically, McGrathNicol raised the following questions for each scenario:

(a) What do you make of the scenario?

(b) Is the scenario likely / realistic?

(c) How would you [participants] be required to respond to this scenario?

(d) How would you [participants] respond in reality?

(e) Is the response any different to how Crown would have responded three years go?

13.4.3 Eleven scenarios were presented to the On-the-floor focus groups, five of these scenarios were also presented to the AML/Compliance focus group. The scenarios covered a number of different money laundering typologies which hypothetically could occur within a casino. The typologies were identified from reports such as 'FATF Vulnerabilities of Casinos and Gaming Sector' and Crowns red flag indicator documentation.

13.4.4 Focus group participants generally agreed that the scenarios presented were reflective of situations that could occur or have occurred within Crown casino. Overall focus group participants understood what was happening in each scenario and identified the money laundering typology that was occurring.

13.4.5 Focus group participants showed an awareness of the controls in place which would aid in either deterring the behaviour from taking place or aid Crown staff in detecting this behaviour. Focus group participants were able to communicate their reporting obligations in each scenario when it was required.

13.4.6 Specific controls in place identified by focus group participants included the following:

(a) Transaction threshold reports (TTR);

(b) Source of Funds Policy (SOF) and transaction limits;

(c) Surveillance ability to identify whether gaming activity took place;

(d) Patron identification (PID) files created where a patron does not have a Crown Rewards card;

(e) TRT cash thresholds;

(f) EGM cash thresholds;

(g) EGM transaction history;

(h) Use of UARs;

(i) Crown rewards card rated play records; and

(j) KYC identification requirements and controls at the Cage.

13.4.7 Appendix H details all scenarios covered within each focus group and McGrathNicol's observations in relation to each scenario.