PRIVILEGED AND CONFIDENTIAL

The following paper (the **Report**) is prepared for the purposes of providing legal advice and is subject to legal professional privilege. Please do not distribute without prior written consent.

CROWN MELBOURNE LIMITED

(ACN 006 973 262)

100 DAY REPORT

PREPARED ON AN INTERIM BASIS – DRAFT AND SUBJECT TO FURTHER COMMENT

Prepared by Louise Lane

Group General Manager – AML

Legal

30 April 2018

1 Purpose

This 100 Day Report is prepared for the Chief Legal Officer – AML Resorts, in his capacity as legal officer for Crown Resorts Limited and the Australian Properties (the **Group**) and in his capacity as the AML/CTF Compliance Officer for Crown Melbourne. This Report is prepared to address his request to advise him of observations at Crown Melbourne.

This Report includes limited commentary in respect of Crown Perth.

This Report does not consider the AML/CTF framework or compliance of the Group's investments in Betfair (itself a reporting entity under the Act) or Aspinalls, with the former managed directly by the Betfair business and the latter falling within the remit of the Group General Manager – Compliance and Regulatory. As a member of Crown Melbourne's corporate group, Crown Melbourne can share information with Betfair in limited circumstances.

This report is prepared on an interim basis, is issued in draft, is confidential and privileged and may be updated from time to time.

This report is prepared in light of the current regulatory environment, and what is being seen at the Royal Commission. I note as follows:

- Companies will be expected to not only comply with the law, but be able to demonstrate that compliance; and
- It is expected that there will be a focus by regulators not just on company culpability but the culpability of individual executives.

This Report is prepared with the foregoing front of mind.

Given Crown's brand in the marketplace, there is significant opportunity to enhance its existing AML/CTF framework to act as market leader in this space. Crown should look to exhibit best practice in this area, with reference to how our peers and financial services institutions behave both here and abroad.

It will be less expensive to invest and properly resource this area now, rather than operate in a reactive manner and be otherwise directed by our regulator (or indeed our competitors in their ear) otherwise telling us what they think the ML/TF risk is that applies to our products and services.

In particular, if Crown does not exhibit best practice as it relates to junket operators, then I have concerns that the ML/TF risks attributed to this area of our business will be determined by our regulator and told to Crown, which may have a significant impact on revenue.

2 Executive Summary

As an overarching comment, my review of the business has identified a number of areas where Crown can enhance its existing framework. This will require the business to embrace some change, and potentially shuffle resources.

I draw the following key observations to your attention.

Transaction Monitoring

[redacted] I have requested the IT team compile data to support the view taken by the business that, due to the inability to legitimise funds in this manner, this ML/TF risk is low.

[redacted]

- There is a true sense that we are monitoring "*because that is the way it has always been done*". I am looking at this as part of the Joint Program and how we can better target our TMP to the risks we are seeking to detect and address.

Reporting

- IFTI reporting is conducted out of the VIP Finance team, with compliance reviews conducted by the Compliance team. I am told by the CTRM that, other than ad hoc training from time to time, the CTRM and the AML team has historically had "nothing to do with it". This is a mistake and is being rectified.
- Crown has represented to AUSTRAC on its business profile forms that it provides accounts as an account provider that is an ADI, a bank, a building society or a credit union. This is an error in reporting and was detected by AUSTRAC. **Given this error, and the manner in which the business has been referring to these accounts, it is my recommendation that the business should conduct a review to ensure that all appropriate approvals and exemptions have been obtained. I note this could occur as part of the Crown Wallet discussion.**
- I have been advised by the CTRM that he acts as a post box on suspicious matters filed, supplementing them where relevant but otherwise just "passing them on". The Joint Program will address this and how we communicate patterns of behaviour back to the staff in the form of training (to look for particular activity).

Information technology

- The CTRM has previously operated on the basis that he has authority to approve IT systems changes as they relate to IT, as well as network accounts. This was "the way it had always been done". This changed early April to escalate the approvals process to Senior Management.
- I have been advised by multiple persons that the IT changes of November 2016 have added significantly to the AML team workload, particularly as the CTRM is 'networking accounts' as part of his role. I am not comfortable with him doing this (particularly in light of recent issues across the

business). I am also told that there is a need to tighten who can create membership accounts and who can amend them. I have spoken with Andre and Craig Preston about this exact matter, and they have advised that this is being driven by the business.

- We have had two IFTI issues where Crown has made mistakes lodging with AUSTRAC. I have made recommendations about moving this underneath AML so we can ensure this is done properly and will provide this detail shortly.

Risk (enhanced CDD, customer risk, etc)

- We have overlap with Mary Gioras' team as to ECDD. Work conducted by Mary may or may not form part of the CTRM's review of a customer's risk profile. This offers an opportunity for improvement, including potentially merging the AML and the Credit Control teams. To discuss as part of the Joint Program process.

[redacted]

- It is rare for a decision made by the CTRM on a customer's risk profile to be escalated to Senior Management. This is being addressed through monthly reporting to the AML/CTF Committee.

VIP Finance

- It is evident that junkets are on the minds of state and federal regulators. This requires two actions: (1) better education as to the checks we are running on these individuals, and their key players; and (2) VIP Finance to strictly enforce directives they are given. I have concerns as to the latter, in light of the time taken with Sun City recently, and comments made to me by Indran.
- In the last six months, I have been advised that 58 SMRs have been filed with AUSTRAC in relation to behaviour in Pit 86, for aggregate transactions totalling $16.8 million. I am concerned by comments made to me by Indran about Sun City. It is my recommendation that a full review be conducted into Sun City in respect of customer risk to affirm that Crown wishes to continue to do business with them.
- **VIP Finance has approved customers to repay debt to Sun City in Macau. This account is in the name of employee [redacted] and has $25 million sitting in it. I have not looked at the legalities of this arrangement but it gives me pause from a reputational risk perspective.**

Resourcing

- There is significant overlap between the AML and Compliance teams, resulting in efficiencies and misreporting. I have made recommendations in this regard below.
- I have been informed by staff in both Melbourne and Perth that they are stretched to the limit. My staff member in Perth has advised me that this is causing her to have anxiety. I am looking to help her wherever I possibly can. In light of the potential ramifications of non-compliance, a team of three with overlap and inefficiencies with Compliance is insufficient.
- Other than me, Crown's AML staff members have no formal qualifications to fulfil the role, which has resulted in some key oversights (including the failure to monitor gaming machines above). I would like to start looking at this immediately.
- The CTRM has no documented standard operating procedures, and previous attempts to create these procedures have not been successful (as advised by the Group General Manager – Compliance and Regulatory). I am working with the CTRM on this now. This process is taking time away from other initiatives. Note that the IFTI reporting did not have documented procedures either.

3 How money moves in to Crown – stress testing our services (where are our potential vulnerabilities?)

I have included the following for your information – in light of the recent guidance note on AML/CTF prepared by AUSTRAC for the pubs and clubs industry.

Table Games

How money enters Crown Melbourne:

- A patron may buy in (cash for chips) at a table game for any amount. He or she will be identified for a transaction of $10,000 cash or more and a threshold transaction report will be filed.
- A patron may buy in at a chip dispensing machine (cash for chips) for an amount up to $2,000 in cash. This patron will not be identified.
- A patron may acquire a "Chip Purchase Voucher" or chips for cash, at the Maple Booth. This patron will be identified if the value of the transaction is for $10,000 cash or more.
- A patron may buy in for a poker tournament at the tournament desk (cash for chips). This patron will be identified if the value of the transaction is for $10,000 cash or more. In the case of tournaments, the patron will be identified when we create a Crown Rewards Card for that individual.
- A patron may buy in for poker at the table (cash for chips). The patron will be identified if the value of the transaction is for $10,000 or more.

Each of the above scenarios, save the chip dispensing machine, involves human interaction with Crown Melbourne. Each staff member involved in that interaction has been trained in AML/CTF Risk Awareness Training.

Other than chips, table games do not issue any other form of casino value instrument.

[redacted]

EGMs | TGs

How money enters Crown Melbourne:

- [redacted] This relates to the provision of a designated service. [redacted]

- A patron attends the Cage (in VIP) and acquires a Gaming Ticket (a TITO Ticket) for any amount with cash (cash for token).

A TITO Ticket **cannot be purchased** at a ticket redemption terminal.

Other than TITO Tickets, EGMs and ETGs do not issue any other form of casino value instrument. You cannot get cash from an EGM or an ETG.

Cage

How money enters Crown Melbourne:

- A patron, or a third party, can deposit cash into a patron's Deposit Account. Customer identification will be taken for deposits of $10,000 or more.
- Wire transfer, including from third parties.
- Deposit at Crown's bank, including from third parties.
- A patron can acquire chips (cash for chips).
- A patron can acquire a TITO Ticket (in the VIP area) (cash for TITO Tickets).
- A patron can deposit money into a Card Play Extra account.
- A patron can deposit money into a safe deposit box (for VIP).
- A patron can exchange foreign currency.
- A patron may acquire a Chip Exchange Voucher (cash for chips).

Crown Melbourne will accept deposits into Deposit Accounts from third parties with very limited checks as to whom the third party is and what his or her source of funds is. This is a question of risk appetite, and is addressed in Observations below.

A patron can extract and convert money with the Cage as follows:

- Cash
- Chips
- TITO Tickets
- TT (including outgoing IFTI)
- Direct Transfer (i.e. patron 1 to patron 2)

Potential vulnerability: third parties deposit funds into Crown's front money accounts which may be from an illicit source.

Solution: restrict third party deposits other than from identified patrons (or if the deposit is from a reputable third party bank or licensed provider). This is a significant shift from existing practice. [***Anne: to discuss***]. Continue to file SMRs for all third party transactions for which we cannot identify a relationship.

Potential vulnerability: converting dirty money. i.e. 'Refining' – dealers seeking to convert small denomination bills for large. The Cage is aware of this risk and monitor for it.

Potential vulnerability: are we seeking persons hoard chips in safe deposit boxes on site?

Junkets

How money enters Crown Melbourne:

- A Junket Operator will be established (following approval by Senior Management), and will have a number of Key Players.
- A Junket Operator may, or may not, be extended credit by the business. To be eligible for credit, the Junket Operator **must be a foreigner, and must not be from China.**
- Junket Operators generally operate in Crown Melbourne's high roller rooms and Salons. The Junket Operator may, or may not, be issued with a unique set of Chips and Plaques unique to that room or salon.
- Junket Operators will acquire chips from Crown Melbourne (in this way, Crown Melbourne is providing the designated service to the Junket Operator). The Junket Operator will then distribute these chips to its Key Players as appropriate. All Key Players are identified by Crown Melbourne.
- Except where it is extending credit, or if a Junket Operator or Key Player is from an identified jurisdiction, Crown Melbourne will not seek further information from a Key Player as to his or her source of wealth or source of funds.
- **The above is an established business model and has been operating for some time globally. It is right in the focus line of AUSTRAC and other global regulators.**
- Crown Melbourne has seen recent issues and has identified vulnerabilities with regards to Sun City. These are addressed at section 6 below.

Hotels

- Crown Melbourne conducts foreign exchange transactions for its guests.
- The threshold for these transactions is set at $500, with anything above to go to the Cage. This policy has slipped slightly in recent times, and we are reiterating the requirements (i.e. ID at $1,000) this week.

Crown Rewards Shops / F&B

- Crown Melbourne will accept cash for the purchase of Crown Rewards Cards. Crown Rewards cards can only be redeemed on the premises.
- Crown Melbourne does not presently issue Crown Dollars (Crown Perth does, although they are not extensively used). These ‘vouchers’ permit a customer to acquire a voucher for cash, and then redeem for chips.

4 Observations

#	Relevant Area	Description of Observations	Action Item / Status / Recommendation
1	AML/CTF Program	1. **Risk Management**: The AML/CTF Program for Crown Melbourne, in particular, the preamble to its risk management section, appears not to have been updated for some time. For example, it refers to an EY report (in the context of positive commentary about Crown Melbourne's Program) that was initiated by PBL (pre 2007). Further, the risk section refers to a risk standard has been out of date since 2009. There are key ML/TF risks that have been identified globally (and by Regulators) and are considered by our casino peers that do not show up on our register and do not form part of our transaction monitoring program. Our Program openly states at "specific controls" for certain risks that there are "*no controls under $10,000*" but the program provides that a risk deemed inherently high is now low. This does not logically follow. Further, there are a number of elements of our Program that should be taken to Board level for its consideration as to its comfort level. These include: - Crown's willingness to accept third party transfers and/or deposits without conducting further KYC or other due diligence to understand where these funds are coming from.	The Designated Services Risk Registers for Crown Melbourne and Crown Perth are presently undergoing a review, with feedback from each Business Unit. AUSTRAC (Intelligence Arm – Michael Beard) is aware of this review for Melbourne. The Group General Manager – Risk & Audit has been consulted at each step of the process (on a regular basis), and the latest draft of the Perth document has been provided to the Risk team for consideration and comment. Once finalised (following review by the CLO and others), the Crown Melbourne document will be updated accordingly and each report will be provided to each Business Unit for sign off. CURA questions for Crown Melbourne will be included for each Business Unit in respect of whether, on a regular basis, any update to the Risk Register is necessary due to new product/emerging ML/TF risks. These questions have been provided to Susan C of Compliance Melbourne for her thoughts. The existing process is that Crown Melbourne files SMRs on third party transfers and does not ask further questions on the sending party. The view has been expressed to me is words to the effect of "*this is the bank's job and they won't share the information*".

			Australian banks provide designated services themselves under the Act as 'reporting entities', and the depositor or transferor will in large part be a customer of that bank, and where appropriate, the bank will conduct ID and file threshold transactions and other reports on that customer in accordance with the Act. In this way, Crown's source of funds is the bank and it is appropriate that we rely on the work conducted by the bank in ensuring it knows its customer. **However** - Crown has an obligation to have in place "appropriate risk based systems and controls so that, in cases where one or more of the circumstances in paragraph 15.9 arises, a reporting entity must undertake measures appropriate to those circumstances…" (one of the circumstances at 15.9 includes a suspicion arising). 15.10 sets out a range of measures, including: - Clarifying or updating KYC information; - Clarifying or updating beneficial owner information; - Obtaining any further KYC information including taking reasonable measures to identify the source of the customer's wealth and the source of the customer's funds; - Undertake more detailed analysis of the customer's KYC information, including taking reasonable measures to identify the source of the customer's wealth and funds; - Undertaking more detailed analysis and monitoring of customer transactions, including but not limited to the purpose and expected nature and level of the transactional behaviour; and - Seeking management approval to continue the business relationship. At present, other than looking at the customer's transactional activity, Crown has not historically specifically engaged in any other ECDD activity for third party transfers. Crown Melbourne may well conduct such ECDD where the transfer relates to a junket operator, or a key patron (due to the work conducted by Credit Control). Further, the CTRM has expressed to regulators, including the Australian regulator that Crown doesn't need to understand source of funds/wealth.

		[redacted] [redacted] A report on bill stuffing behaviour on these machines (for instance, drop and collect within a set time period) should be implemented to enhance the AML/CTF Program. Almost all money laundering typology documents prepared by foreign regulators and/or industry groups identify "*bill stuffing*" as one of the key money laundering risks in respect of slots. The Australian regulator AUSTRAC has also identified this as a risk, as recently as	This is not technically correct, but has been the position Crown has taken previously. Whether or not Crown needs to understand source of funds/wealth turns on the position Crown takes under Rule 15.10. **It is my recommendation that the Program be amended to provide that, where a customer receives a third party transfer and that transfer is not from one of the big 4 banks or another reputable provider that is a reporting entity or is regulated under equivalent AML/CTF laws in another jurisdiction, that ECDD be conducted as this constitutes "a measure appropriate in the circumstance". This includes monies from foreign jurisdictions.** The Rules require that Crown Melbourne have a transaction monitoring program in Part A of its Program, that the TMP include appropriate risk based systems and controls to monitor the transactions of customers. Further, the Rules require that Crown Melbourne have a transaction monitoring program with "*the purpose of identifying, having regard to ML/TF risk, any transaction that appears to be suspicious within section 41 of the Act*" [Rule 15.6]. Section 41 of the Act refers to suspicious activity in respect of **"designated services"** not "customers". The taking of a bet, or entry into a game, is a "designated service" for the purposes of the Act [Table 3, section 6, Act]. The $10,000 threshold relates to identification. In discussions with the CTRM since December 2017, and with the Group General Manager – Regulatory and Compliance, the position has been taken by Crown Melbourne that money is not being laundered in this way because the funds are not legitimised as there is no rated play. This is contrary to where Regulators are moving. This ignores the process taken by drug dealers (for example) cleaning money. It has been confirmed to me that STAR conducted a review of 200 of its EGMs last year to assess this risk. This review took 90 days, involved 4.5 million transactions, and I am informed resulted in only one additional SMR.

			February, in a formal publication to pubs and clubs. "*Bill Stuffing*" is where a patron goes to various slot machines putting cash in the note acceptors (bill acceptors), collects TITO tickets with nominal activity, then cashes out at the Cage or asks for a cheque.	I have raised obtaining reports with Kierren Gersbach and the EGM team to address this issue (the latest discussion 20 March 2018 in which I relayed the STAR information to Mark Mackay in the context of we should be looking at conducting same and that we presently have very little in the way of transaction monitoring of the machines, as distinct from 'customers' who are otherwise ID'd). The purpose of this report, and regular reporting, will be to satisfy ourselves that this designated service is not being misused, and if it is, that we are reporting that suspicious behaviour and that we update our TMP appropriately. **UPDATE: this is in train – report to be obtained from CDW for all machines with a daily aggregate buy-in of $9k+ to understand risk (with a ratio of 1:10 | Turnover: Buy In). The report will be generated by IT and reviewed by the GGM-AML.** Acknowledging the above as it relates to EGMs, please note that the current policy of Crown Melbourne is as follows: - Crown Melbourne does not monitor drop on EGMs or ETGs. - A patron can insert, in one go, up to $9,899 (the **Note Acceptor Limit**, and then a further $100 to $9,999) in a machine, play it, hit collect and then take a TITO ticket to the Cage. If the patron has played a restricted machine, he or she will be issued a cheque (for which standard practice is to provide CID to ensure that the patron is the payee) and the balance in cash. If playing an unrestricted machine (whether in unrestricted mode or not), the patron can collect a TITO, exchange it for cash up to $9,999, without providing any form of ID. - **I am told that a patron can also insert up to $9,899 and then insert a TITO Ticket for any amount (the note acceptor limit relates only to cash). The business has been unclear as to what exactly happens here. Please note that action is required here.** [redacted]

		- The level of [redacted]	[redacted] This position is consistent with and meets the requirements of the Act and Rules [redacted] - Crown Melbourne updated the manner in which patrons can [redacted] • [redacted] • [redacted] • Crown may well have [redacted] • **Relevantly**, the patron cannot [redacted] • The risk here is that the patron that [redacted]

			[redacted] we are not generally seeing this. [redacted] – that is, [redacted] - Crown Perth [redacted] **This can be viewed two ways:** [redacted] [redacted]
		- The issue of Deposit Accounts versus Betting Accounts and how we monitor activity on these accounts.	Crown Melbourne (and Crown Perth) has disclosed to AUSTRAC for many years (via its Business Profile Form) that it provides its deposit account in the capacity of an account provider under the 'financial services' section. This was due to a misunderstanding and an unclear Business Profile Form, and this has been raised with AUSTRAC. It is arguable that the Deposit Account and the Cashless Accounts are not 'accounts' for the purposes of the Act, for an account is defined as: *"includes:* *(a) A credit card account; and* *(b) A loan account (other than a credit card account"; and*

			(c) An account of money held in the form of units in: *(i) A cash management trust; or* *(ii) A trust of a kind prescribed by the AML/CTF Rules.* *To avoid doubt, it is immaterial whether:* *(d) An account has a nil balance; or* *(e) Any transactions have been allowed in relation to an account."* "Betting account" is undefined, and there is no Guidance Note. For Act/Rules compliance, Crown has assumed that the Deposit Account is an 'account' for the purposes of the Act, and we comply with the requirements of this being a "designated service". A review of the 'deposit accounts' gives rise to areas requiring further inquiry: - How does Crown Melbourne account for the monies deposited? Are the funds held on trust for depositors and if so, how? - On what grounds is Crown exempt from the requirements of Chapter 7 of the Corporations Act or otherwise what exception applies to Crown that these deposit accounts are not subject to banking / other laws? - The AML team infrequently checks deposit accounts for monies 'parked'. It is clear these accounts are for the purposes of gambling. **Proposed Resolution:** I am working with Cage to get a report on this on a regular basis. - There is little to no oversight of the Cashless Product other than where a deposit or withdrawal is made of $10,000 or more in cash – i.e. Card Play Extra and this 'account' is not addressed in the AML/CTF Program (nor is it referenced in Crown Perth's AML/CTF Program). **Proposed Resolution**: update the Program to reflect this account, and am working with Peter Dawson to understand what reports are available to us to monitor

		- Crown's credit policies and the means of repayment of debt from offshore.	Where Crown provides "credit" to foreign VIP customers, it is not clear whether Crown Melbourne has considered whether this is a 'loan' for the purposes of the Act [Item 48, Table 1, section 6 Act]. Crown is finding it increasingly difficult to repatriate these funds from overseas jurisdictions, and this situation is not improving: - Patrons are including on transfers "investment property" or "investment". We are being told that this is due to the banks or licensed remitters improperly including this reference due to the name of our account to which the funds are being transferred ("**Southbank Investments**"). Where patrons have sought to include "investment property", the instruction from AML has been to send the funds back. Extended discussions with Roland Theiler that Crown Melbourne cannot accept funds where it appears the patron has inserted the incorrect description. **Resolution: email to Roland Theiler advising "investment" is OK provided we can substantiate details of the funds and that they are only used for gambling (or in certain scenarios, to repay a loan where the funds the subject of the loan were used for gambling). "Investment for property" will not be approved and the funds must be returned.** - Patrons are seeking to repay loans via third party companies. Crown is unable to ascertain the association between the patron and these companies, necessitating those funds to be returned. VIP Finance continue to press that Crown Melbourne be permitted to accept funds from companies 'connected' to licensed money changes. Thus far, the answer to that has been 'no'. STAR has advised in April they are having the same issues. - Of late, we have seen the following transactions of a patron seeking to repay a debt (or for gaming):

			• The carrying of more than $800,000 on Crown's private jet by a third party on behalf of a patron. • Funds sitting offshore with Sun City in Macau, in repayment of debt. • A deposit of $816k to ANZ Swanston Street from an unknown third party into the Southbank Investments account for a [redacted] then advised that he was not able to play and requested the funds be wired to him in Hong Kong. This request was declined. Subsequent KYC has determined that the person depositing the funds was a 'friend' of [redacted] **Recommendation: in respect of our bankers, that we require deposits in excess of an agreed amount (following a risk assessment) require Crown Melbourne approval where the deposit is a third party deposit and the customer is not a customer of the bank.** • $12.7 million repaid by [redacted] to Crown through multiple third party accounts. Crown has been unable to connect any of these accounts to this individual. [redacted] is well known to Crown, and well known to the Australian government and Australian press. https://www.smh.com.au/national/chinese-king-of-the-mountain-brush-with-corruption-scandal-20160224-gn2tvt.html **Recommendation: a compliance review should be conducted as to all credit arrangements in place, to ensure that policy is being strictly followed.** **Comment:** In the event that this is a designated service, Crown Melbourne complies with its obligations under the Act (in that it conducts CID, it conducts further KYC, it conducts ECDD where relevant, it monitors transactions relevant to the loans and it reports SMRs where they arise). This is a matter of updating the AML/CTF Program appropriately to reflect the above.

		- Whether Crown is comfortable entertaining customers from prescribed foreign countries. Since 1 September 2017, 124 Iranians and 140 North Koreans (per their passports) have visited Crown Melbourne.	Iran and North Korea are 'prescribed foreign countries' for the purposes of the Act. Crown Melbourne has recently amended its AML/CTF Program to take into account other countries listed by DFAT for the purposes of its customer risk analysis. Since 1 September 2017, Crown Melbourne and Crown Perth have seen (in aggregate): - 124 Iranians; and - 140 North Koreans, join the Crown Rewards program. The Act provides that regulations may prohibit or regulate the entering into of transactions of prescribed foreign countries (Iran, North Korea). Historically, the Regulations provided that reporting entities should not conduct transactions with Iranians over $20,000. This was communicated by Scott Howell to the business on 10 June 2016 and, notwithstanding the Regulation was repealed we have continued to adopt this position for ML/TF risk mitigation purposes. Crown Melbourne and Crown Perth continue to entertain patrons who are from prescribed foreign countries, designating each patron as a 'high risk'. It may be that Crown remains comfortable with this approach however it would be my recommendation that these patrons have their customer risk increased.
		- Jurisdiction risk – Chinese patrons	Crown Melbourne's Credit Control team is conducted enhanced KYC and customer due diligence on Chinese VIP patrons, yet this is not formalised in any formal documentation. Consequently, the AML/CTF Program is out of step with existing practice. **Recommendation: Update the AML/CTF Program, and ensure that all Chinese VIPs are appropriately risk rated from an ML/TF perspective.** **Update: memo to JP regarding conversation with Roland April 2018.**
		- Source of Funds / Source of Wealth	Please see my comments above with respect to third party transfers and rule 15.10.

			Recommendation: Crown Melbourne's ECDD processes should be updated to be made clearer as to when source of funds information is sought under Rule 15.10(c) and 15.10(2). This should include where: - **A patron is from an identified jurisdiction.** - **The amount is greater than a determined sum (for instance, $100,000).** - **The patron otherwise exhibits unusual or suspicious behaviour (multiple cheques, unexplained changes in play).** - **The patron seeks to repay a debt through an unapproved method (for example, through a third party company).** **The source of funds / source of wealth checks would be conducted as follows:** - **A wealth insight or C6 report (or another equivalent report).** - **Google research.** - **Discrete enquiries of the Junket Operator.** **These checks are currently occurring, although not as general practice. The CTRM should be instructed that these checks are to occur, that they be documented and that the customer's risk profile be updated accordingly.**
		2. The CTRM, tasked with implementing the AML/CTF Program, has confirmed that he has not read it in any detail – I am told by the Group General Manager – Compliance and Regulatory this is due to the former structure when the Program was controlled by the former General Counsel of Crown Melbourne.	**This is not a suggestion that the CTRM is not across the detail – he largely is.** GGM-AML to provide CTRM with a training session on the requirements under the AML/CTF Program (that is, to take him through each section and allow him to ask any questions or make comment if he thinks it is wrong). For instance, CTRM was not conducting source of funds/source of wealth checks on foreign PEPs, which is a requirement of Rule 4.13.
		3. The CTRM has no standard operating procedures (other than the broad parameters in the AML/CTF Program, which are ambiguous), making an audit of his work (which is acknowledged is considerable in terms of work load), difficult and makes	Under development, in line with Perth. I am told that discussions to develop this previously have been unsuccessful. That will not be the case here. Please note that this is not a suggestion that the work is not being completed, simply that it is not simple for Crown to point to this work. This

		reporting to a third party challenging. This is important as Crown Melbourne must be able to demonstrate the various actions taken by the CTRM (and others) under the Program is occurring. At present, this is not an easy process. Case in point: CTRM has identified he "*is not responsible for IFTIs and wouldn't have a clue whether we are compliant or not*". This is a matter of Program compliance and hence should sit within AML's remit.	makes assurance difficult. The purpose of the SOP for Crown Melbourne is to: - Align with Perth, in advance of a Joint Program; and - To ensure it is easier to describe what the CTRM does, how he does it, why he does it and what he discovers. The AML/CTF Program for Crown Melbourne as presently drafted is needlessly complicated and difficult to describe to newcomers and to regulators, when that need not be so. A consequence of the CTRM not being "across" the IFTIs is the SOP has not been updated since 2008. **UPDATE: On 17/4, Crown Melbourne became aware of another issue with IFTIs, with a mistake made on 55 lodged forms. This is twice in six months. See email correspondence. It is known that we have had IT issues and the VIP Finance team were not checking lodgements. Rectified.**
		4. The current customer risk analysis is conducted by the CTRM and a Compliance Manager. The record of a customer's risk assessment (**which is not referrable to any concrete risk parameters**) is presently recorded in the C drive of the CTRM. Only foreign PEPs are escalated to Senior Management for approval.	Crown Perth retains customer risk information in CURA. Crown Melbourne is presently undergoing a rollout of this software and this will be included in this rollout. The AML team will require assistance from IT, or a temp, to ensure that the existing customer risk profile and history is appropriately updated to CURA upon rollout. In the interim, I am working with the CTRM to move this information out of his personal files and in to a G drive.
		5. The customer risk analysis is arbitrary (largely, at the sole discretion of the CTRM) **and not available to front line staff nor senior management on any regular basis**.	Initial discussions have commenced with the CURA roll-out team as to how we ensure this information is appropriately transposed. This is a discussion item for automation and the development of appropriate business rules.
		6. The Program does not distinguish properly between ECDD and obtaining additional "KYC" Information. There is no suggestion	Adopt Crown Perth's language (which better delineates between the two). This change is to be marked into the AML/CTF Program, and Crown Perth's language is to be included in the Joint Program.

		that Crown Melbourne (and the CTRM in particular) does not understand the difference – simply it is not sufficiently clear in the Program.	I note that the differences in language between the two Programs appear to have been due to discussions with the regulator from the inception of both programs, which were built off the same pro forma.
		7. The CTRM is tasked with the responsibility of monitoring attendance of Refresher Training. This oversight has not been done in a complete manner. Business Lines are providing additional training on AML/CTF matters without materials sighted by AML (or recorded by HR as to the training conducted). This is leading to an undersell of the amount of AML training conducted by/with the business.	This has been taken on by me, and I am working with Shane Thomas on attendance rates and communication. The low attendance rates have been discussed with Sean Knights (in particular). It has been confirmed March 2018 that the Group General Manager – Compliance and Regulatory is to include this item on the agenda of meetings with EGMs and Table Games on a monthly basis, and report back to me on compliance with the AML/CTF training requirement. **This change has been implemented, and compliance rates are improving (now at 91%). Making clear that 100% is the target.**
		Additionally, Crown's AML/CTF Training is due a refresh, and should be targeted to each business line.	In development. First set of targeted training to Hotels 4/4/18. Workplace instructions updated.
		8. PEP screening – Crown Melbourne (and Crown Perth) presently use Thomson Reuters, and a software provider Fircosoft (which 'washes' our database against Thomson Reuters for PEP and other checks). Comments:	
		- The definition of "active" customer was incorrect and consequently, screening was narrower than anticipated.	**Detected and now corrected**. As a result, the 250,000 screening number for Thomson Reuters has been underestimated and we may well expect additional costs from Thomson Reuters. Once we understand the impact on the additional customers to be screened, I will be able to confirm on expected additional costs and appropriate solutions.
		- Fircosoft takes 28 hours+ to screen our database. It is unclear whether this is a Crown or Fircosoft issue. The internal cost to the business of seeking to rectify issues with Fircosoft is extensive (1 AML resource; 1 IT resource).	Detected and working with Fircosoft to rectify. Previously, advised that PEP screening daily, which is not correct. This requires a change to the Crown Perth AML/CTF Program to clarify. We continue to comply with the Act/Rules. This is budgeted (by IT) and an email has been sent to Inez and Quintin

			sent 27 March 2018 to push the process along, after consultation with Ben Briggs and after the most recent failure of Fircosoft. RFIs distributed by procurement in April. This is well underway. **Resolution: this project will form part of the broader project for ABCC and screening of suppliers. Emails with Sasha, Anne and others early April to ensure that the PEP screening program dovetails in behind this work and we seek to gain efficiencies through the use of one provider. This is in train.**
		9. IT issues – as raised by Claude, the existence of multiple accounts for patrons has added to the workload of the CTRM (and the Legal Officer – AML in Perth). Specifically – if an SMR is received in respect of patron X, the AML team will often check two or more additional Crown Rewards numbers to ensure the information provided on the SMR is correct (for example, as to win/loss/turnover on an aggregate basis). This also complicates disclosures to law enforcement agencies.	This matter has been escalated by Claude in March 2018. Claude has confirmed he will advise me of the outcome. The IT worklist indicates that this matter will be resolved by the end of this financial year. Confirmed by Jasmeen Grover week of 16/4 that this will be resolved by first quarter FY19. **Email to JP of IT issues as it relates to networking on 19 April 2018.**
		10. Foreign exchange transactions are conducted by hotels up to A$500 (with higher transactions sent to the Cage). Hotel staff receives limited training.	Crown's hotels conduct foreign exchange transactions, which is a designated service for the purposes of the AML/CTF Act. Hotel staff does not attend the same training as front line staff in the Casinos (involved in the provision of designated services). Given the infrequent nature of the provision of this designated service, and that CID is not required (as the threshold of these transactions at $500 is below the $1,000 in the AML/CTF Rules), I have updated the Hotels Workplace Instructions to address: - What is AML/CTF and why it is important; - What Crown's reporting obligations are; and - What to do if you see something suspicious (who you report it to, what you report, not to tip off), tailored for the hotels / foreign exchange. I will also provide targeted, brief training as required by the hotels business.

		11. Upon commencing with the business, there was some ambiguity as to whether or not Appropriate ID should be taken when establishing a Crown Rewards membership (as a membership is not a designated service for the purposes of the Act).	The Crown Rewards Rules make clear that Appropriate ID is required by Crown. This has been made clear and has been reinforced to Crown Rewards staff members. This will be important when commercial initiatives are to be rolled out that otherwise require Appropriate ID (for example, if Card Play Extra were to be rolled out more broadly, and in anticipation of Crown Wallet). Please note that deposit TRTs contemplate the use of a PIN to deposit funds. The deposit functionality has been placed on hold at this time. However, in the interim, a check should be conducted to ensure that all Card Play Extra cardholders have Appropriate ID on file. **Recommendation: this has been raised with Michelle Fielding and Mark Mackay week ended 30 March 2018 – indicated happy to help. This will be an important check going forward to give a snapshot in time.**
		12. The Crown AML/CTF Program has been outstanding, pending the changes put to AUSTRAC in October 2017. A series of AML/CTF Rules were released in January (and with which Crown is complying), that should be built into the Program.	Agreed with Barry Felstead that Crown Melbourne (and Crown Perth) will update their respective policies. To be provided this week.
2		**Act and Rules** 1. Crown Melbourne (and Crown Perth) needs to examine which services it provides fall under which 'designated service' under the Act.	This is underway. The differences in approach between Crown Melbourne and Crown Perth will be rectified by the adoption of a Joint Program under the Act, which is presently in draft form. The adoption of a Joint Program has been supported by AUSTRAC. **First draft of Joint Program largely completed. Deadline 31/8.**

		2. Crown Melbourne gives front line staff discretion as to whether or not to accept ID for a cheque issuance of $10,000 or more (although noting that standard practice is to ask for Appropriate ID per Stephen Hancock and as advised to AUSTRAC).	This has been raised with the Group General Manager – Compliance and Regulatory and with Chief Legal Officer on 26 March 2018. This has also been raised with the Group General Manager – Risk & Audit from a Rule 10.1.6 perspective (risk management). **Update: LL to speak with DV upon her return from leave to understand historical view.**
		3. The Rules require that, for 'high risk' patrons, ECDD is conducted. Crown's systems make it difficult to determine if, and how, the ECDD has been conducted.	Crown Melbourne is conducting ECDD on patrons however it is difficult to demonstrate. Indeed, there is some argument that the CTRM is conducting ECDD on customers every day, which may not be entirely necessary. The Regulator has regularly raised ECDD as a point of concern for Crown Melbourne. As recently as January this year, the intelligence team has requested the additional information we obtain on particular patrons (C6, Wealth Insight). The extent of ECDD has improved since December 2017, with ECDD clearly noted by the CTRM against the relevant patron's SYCO details.
		4. Crown Melbourne has a number of reporting obligations under the Act, including: - Reporting threshold transactions; - Reporting international funds transfer instructions; and - Reporting suspicious matters. The present means of assuring senior management that every transaction is being recorded can be improved. The consequence of a failure to comply with these reporting requirements is severe. The current assurance format, from September 2017, moved the assurance function from the AML function to the Compliance function. This needs to be made	**<u>Threshold Transactions</u>** The current SYCO system does not preclude a staff member from entering a threshold transaction without requisite ID (i.e. a non-compliant TTR). Instead, our controls require that a senior manager 'double' behind the staff member. At or about September 2017, the responsibility for conducting spot audits on various compliance matters to do with the AML/CTF Program was shifted from the CTRM to the Compliance team. I understand that the timetable has been established in conjunction with Compliance requirements, in the ordinary course. **There is no audit of threshold transaction compliance, other than the daily checks conducted by the CTRM and the Compliance Manager (which are for completeness, not for compliance with SOP).** The matter of spot checks of TTRs has been discussed with Justin Butler and Karyn Barbati in March, however remains an outstanding matter (and

		clear in the Program, and to Compliance.	is not on the compliance calendar). It would be useful that a spot audit confirm that Crown Melbourne continues to comply with its obligations. We are complying with our obligations. A failure to comply has serious penalties under the Act. **Recommendation:** **1. Include spot checks by AML/Compliance on SOP compliance immediately on a quarterly basis, with reports of these spot checks to be provided to senior management.** **2. LL to review previous extraction reports approved by AUSTRAC as a cross-check of ongoing compliance (that is, check the fields in the file against the requirements of the Act and Rules).** **<u>International Funds Transfer Instructions</u>** The reporting of international funds transfer instructions is presently conducted by VIP Finance. In February 2018, the EGM of VIP Finance, Roland Theiler, indicated to me that he was concerned that his staff have not had sufficient training and do not have sufficient bandwidth to ensure that these IFTIs are reported properly. This was relayed to JP. Crown Melbourne has already had an instance of non-compliance, which was rectified appropriately. The CTRM has repeatedly advised me that he is not aware whether or not Crown Melbourne complies with these sections as this doesn't fall within his remit. As noted above, the responsibility for spot checks was shifted from the CTRM to the Compliance team at or about November 2017. These IFTI checks are conducted twice per year. The last check was January 2018. **Recommendation: CURA include a compliance certificate requiring VIP Finance to sign off the team is meeting is obligations. My preference is to bring this function underneath AML in order to**

			control this process (and to give the Board complete comfort as to compliance as at present, I am one step removed and cannot give that assurance). The consequences of failing to comply are too serious for your AML team to advise that it doesn't know anything about it. **Update: another issue 17/4. Again discussed bringing IFTIs under AML but insufficient resourcing to enable us to do that – understandably, have to rely that the business will follow its processes. GGM-AML to review workplace instructions and sit with VIP Finance for next three lodgements to make sure following process.** **<u>Suspicious Matter Reporting</u>** The existing practice at Crown Melbourne, implemented by the CTRM, is that he automatically lodges any suspicious matter forms. In this way, akin to a post box. This process since end November has been enhanced by: - The CTRM receiving the Surveillance and Security reports (previously not received, unless forwarded by Group General Manager – Compliance and Regulatory). - The CTRM receiving a monthly listing of WOL's (previously not provided in this format). - The Surveillance analyst team (Radek Stopka) assisting in various assessments (EGM usage and TITO ticket redemption at cage spot checks). This team is now clear on our reporting obligations under section 41 (see email 15 February 2018). - Where relevant, cross-pollination of activity across Melbourne and Perth. - The CTRM briefing the AML/CTF Committee on SMRS filed and what he is seeing. - The GGM-AML briefing security and surveillance on patterns of behaviour seen, and commencing to provide direct feedback on SMRs lodged. As the AML Program continues to mature, a top-down, bottom-up risk management strategy can be rolled out (consistent with the broader Crown risk management framework). This will enable Crown to assess the

			suspicious matters reported by its front line staff, review its controls and communicate the update to the business. This is not presently formalised.

		5. "**Deposit Accounts**". Accounts under the AML/CTF Act and Rules require Appropriate ID at the time of the account opening, and upon deposits and withdrawals. Crown Melbourne has, to date, indicated to me (and to AUSTRAC) that it has two accounts: - The casino management / front money account (Deposit Accounts); and - The Cashless Account (aka Card Play Extra, aka EzPay (the system upon which it runs)), allowing **external** transfers and deposits onto the Card.	A PIN will be appropriate where Appropriate ID is already on file (although note we will need to update the AML/CTF Program) [section 32(1)(b); section 34(1)(c)].
		SOPs then refer to other accounts, including Safe Keeping Accounts, which I understand to sit adjoining a Deposit Account, and are not used to facilitate betting (this is done through a Deposit Account).	This information has not been disclosed to AUSTRAC, as was provided to me following the Compliance Assessment. I have been told by the business that they are one and the same. **Comment:** 'accounts' are referred to by differing names across the business, which complicates the understanding as to what applies to what. Patricia Chin **(IT)** is presently working on 'governance language' – **it is recommended this be caught in that consideration and/or I complete this process separately.**
		Crown has an additional functionality on its Crown Rewards product called "Card Play". This functionality allows customers to collect credits from EGMs onto the Crown Rewards card, and then use these credits at other EGMs (with the Crown Rewards Card effectively acting as a TITO ticket). The only means by which a customer can receive a payment of winnings is via collecting a TITO at the Cage. In order to move money on an EGM (upload onto Card, download onto EGM), the patron must enter a PIN. It is unclear whether Crown presently conducts any monitoring of the movement of	The relevant consideration for this product, from a risk management perspective, is that it facilitates a patron inserting upwards of $9,899 into a machine, hitting collect, entering a PIN and then transferring the cash into credits, to then move from machine to machine. It has been suggested to me that some accounts do not have Appropriate ID. This should be rectified immediately or the PIN should be disabled (thereby triggering the relevant patron to attend the Crown Rewards desk and reset their PIN, which requires the provision of Appropriate ID).

5 Other Critical Observations

1. **VIP International**. The following activities have been conducted which give rise to potential ML/TF concerns. These actions were taken without prior reference to the AML/CTF Committee:

   - Third party transfer of cash on Crown's private jet. Potential issue: source of funds, incorrect disclosures at the Border (the responsibility of the patron). Why were funds not deposited in an account in the departure country?

   - Deposits by debtors into an account with Sun City, ostensibly to repay debts owed to Crown. These funds remain in Sun City, and it remains unclear whether these funds are held on trust for the depositing parties (which is my understanding) or held as agent of Crown Melbourne. **In any event, the funds are in the name of Ricky Lee.**

     The ML/TF concerns here are that Crown has no clarity as to the source of these funds (only that they are not from winnings and are not front monies), and is on notice that banks in the jurisdiction otherwise will not otherwise transfer them to Crown. Crown Melbourne has historically dealt with, and conducted ECDD upon, CCW (not the corporate entity). **Recommend we conduct ECDD on Sun City corporate.**

     Broader than this: Is Sun City reporting to its regulator that it is holding these funds for Crown Melbourne, and our view at this end is that they are held for customers and that the debt is not repaid? I cannot get a clear answer from Roland on this.

     My concern here is the reputational risk (amongst others) of Crown Melbourne having a fund sitting offshore in the name of an employee, and nobody knows how it works - is it held by SC on behalf of the parties paying the debt, or do they hold it for us? I appreciate I am not across the detail discussed. These style arrangements are identified as high risk.

   - Completing customs forms for high risk patrons. Crown Melbourne should have its eyes open to the risks associated with undertaking this activity, particularly as it relates to disclosure of cash (as movements of physical currency into or out of Australia must be disclosed under the AML/CTF Act).

   - I have received numerous comments from across the business raising concerns about Pit 86. From October 2017, 58 SMRs have been lodged in respect of that room, for cash transactions totalling $16.8 million.

   - Scott Howell conducts customer risk assessments for Crown Melbourne. Mary Gioras conducts risk assessments (of sorts) for junket operators and other key patrons. There is no overlap, the ECDD conducted is not noted in SYCO, potential overlap of role and responsibilities, and that the AML/CTF assessment of risks is not capturing the work (and otherwise risk assessment) of the business.

2. **IT**. On and from October 2016, the AML/CTF Team has been addressing multiple issues with Crown accounts, including:

- Multiple patron accounts – transaction monitoring. This impacts AML/CTF as, when conducting transaction monitoring, Crown will review a patron's rated play, as well as other relevant information, to determine whether to file a suspicious matter on the individual. This is a material issue which remains outstanding. **It is scheduled to be corrected Q1 2019.**

- Networking of customers. At present, Scott Howell as part of his role will 'network' accounts that he identifies relate to the same patron. He has advised me that these accounts are then 'delinked' by other staff members. Two points:

  - I am concerned that Scott's focus on networking accounts may otherwise distract him from other (more important) elements of his role;

  - It serves no purpose if there are no strict rules around who is able to establish accounts, which person is able to network them and how.

  Please see my email of 19 April 2018.

- Any staff member can presently create a customer account. I am informed that a staff member can change a customer's account, including as to their KYC information (per Jimmy Rousis, Thursday 12 April 2018).

  Other than obvious integrity issues, this gives rise to situations where a customer may have two accounts, one a primary and one a secondary, with staff altering which is the primary (for instance: Louise Lane GM account established for me as a gaming machines client).

- **Approvals**. Crown currently files a number of reports to AUSTRAC in accordance with its statutory obligations. We have now had two IFTI issues where updates have been approved in the system and have resulted in incorrect disclosures due to "glitches".

  Solution – approvals must come from the GGM-AML, via the AML/CTF Committee when it impacts a reporting obligation. This was communicated 6/4.

- **PEP Screening:** Crown Melbourne (and Crown Perth) currently screens its active customers multiple times a week, through the use of a software provider, Fircosoft. The following issues have been identified and, where noted, rectified since I commenced:

  - All internal parties had been acting on the erroneous assumption that an 'active customer' caught all relevant 'active' actions. The definition upon inspection did not. It has been fixed.
  - Fircosoft implemented a major upgrade in December 2017 without prior consultation (or perhaps consultation may have occurred as it always had). No clarity was provided as to what the new algorithms would mean from a compliance and IT perspective, only that Crown should just "enable them". When Crown asked for further detail, it was told that this required additional work from Fircosoft and that Crown would be charged for it (with Fircosoft pushing a "health check" on to Crown quite aggressively). This health check will be at an extra cost.
  - Fircosoft collapsed in February / March, requiring IT to implement a workaround.
  - Fircosoft takes 28 hours to screen Crown Melbourne's active customers. Fircosoft cannot explain why.

Solution – RFI commenced to find alternative provider. Led by Procurement. Fircosoft currently screening. LL has reviewed algorithm changes, set up meeting with Jasmeen week commencing 23 April and, subject to getting JG comfort, to enable a number of the disabled algorithms to address increase in false positive results.

- **Fircosoft:** introduced a new set of algorithms that radically increased the number of false positives to the AML team.

  Solution – Algorithms reviewed, instructions given to IT, to resolve.

- **EGMs:** This area of the business is inclined to roll out a process where it has otherwise been advised that it must obtain AML approval. Case in point: the proposal to switch on Card Play Extra when expressly told 10 April 2018 not to without AML/CTF and JP approval.

3. Transaction Monitoring Program (ongoing customer due diligence, or OCDD)

As noted above, the AML/CTF Rules require that Crown Melbourne must:

- Have in its AML/CTF Program appropriate risk based systems and controls to enable Crown Melbourne to determine in what circumstances it needs to obtain further KYC (know your customer) information about a patron, to enable the review and update KYC information for OCDD purposes.

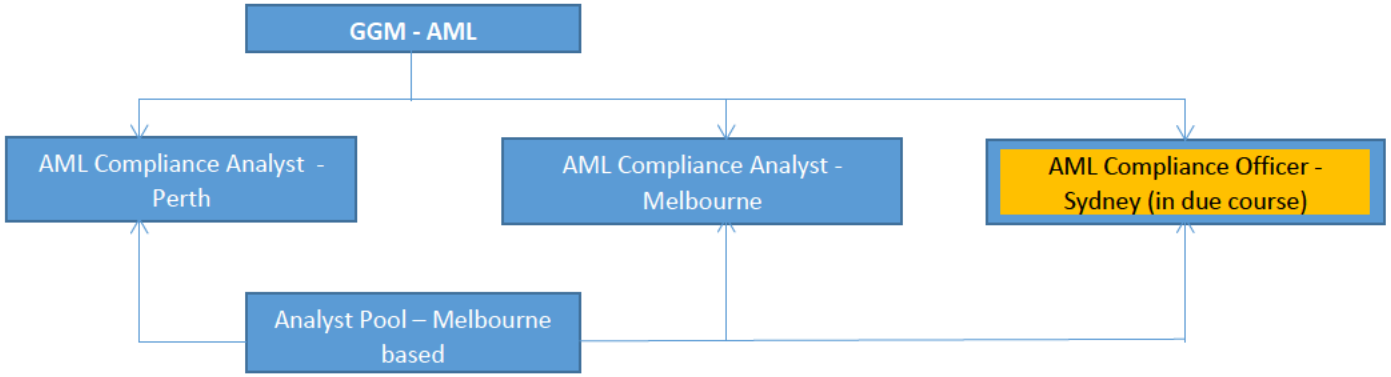
- Undertake reasonable measures to keep, update and review the documents, data or information collected under the applicable CID procedure (particularly for high risk customers).

- A transaction monitoring program that includes 'appropriate risk based systems and controls' to monitor the transactions of customers. The TMP must have the purpose of identifying, having regard to ML/TF risk, any transaction that appears to be suspicious within the terms of the AML/CTF Act. The TMP must also have regard to "complex, unusual large transactions and patterns of transactions, which have no apparent economic or visible lawful purpose."

This was addressed above, and is a work in progress with the CTRM.

6. Resourcing recommendations

In March, I recommended the following structure (sitting immediately below the AML/CTF Compliance Officer).



Each of the compliance analysts should be CAMs certified (Association of Certified Anti Money Laundering Specialists). This costs approximately $2k per person. I have already achieved certification, for me it will be a matter of recertifying.

The GGM-AML role is currently critical as we work through the review phase of the AML/CTF Program. Specifically:

- Review of the AML/CTF Program in Melbourne (and where relevant, in Perth).
- Addressing key elements of the AML/CTF Program and efficiencies.
- Preparation and implementation of the Joint Program across Melbourne and Perth.
- Investigation and implementation of an automated solution for Crown's transaction monitoring.

The current timeline to implementation of a Joint Program is as follows:

1. Review by Minter Ellison of the Crown Melbourne AML/CTF Program – May / June 2018.
2. Development of the Joint Program framework – by 30 June 2018.
3. Implementation of Joint Program – by end August 2018 (AUSTRAC discussions permitting).
4. Investigation of automation of elements of transaction monitoring program – by December 2018, to implement in CY19.

Calendar Year 2019

Following the end of December 2018 (and most likely from mid-2019), it is my current expectation that:

1. Provided the compliance officer positions are properly filled, and all things being equal, the GGM-AML role may then be a part-time role, could be expanded to cover financial crime more generally (as is seen more commonly), **could be shifted to be a dedicated resource for VIP International (my recommendation) or** - if that is not appropriate – could be made redundant.

   The part time role **could** be filled by Brett Hereward, with Betfair's program then being pulled into the Designated Business Group, using the same analyst pool.

2. The analyst pool, funded by reallocating resources in Melbourne, performs the grunt work currently undertaken by the existing AML officers, freeing up the Compliance Analysts at each site to focus on the Program and to be business-facing in ML/TF risk assessment.

   The analyst pool may also provide additional time for the Compliance Officers to take on tasks traditionally performed by other departments (for example, ECDD), which may offer opportunities for efficiencies and head-count reductions in other departments. This could include IFTI and other reporting, resulting in a decrease in head count from another team.

3. By removing the reliance on Compliance and Regulatory, this then allows those employees that currently support the AML team (Sean Counihan, Karyn Barbati) to focus on their day-to-day tasks, and alleviates pressure and double-work. This might also offer some opportunity for resourcing analysis and reallocation in that team.

4. The analyst pool might be a shared resource across risk more generally (reporting to the AML/CTF Compliance Officer and GGM – Risk and Audit), and could assist in reviewing false positive alerts in respect of the screening of vendors (under the ABCC program).

Ends.

ANNEXURE A

Overview of AML/CTF at Crown Melbourne

The current AML/CTF structure at Crown Melbourne is described below. Where relevant, I have included considerations raised by AUSTRAC relevant to the pubs and clubs sector (released in 2018):

1. **Reporting Entity**: Crown Melbourne is a reporting entity under the AML/CTF Act and AML/CTF Rules. Crown Melbourne provides designated services under tables 1 and 3 of the AML/CTF Act, that is – we provide both ***gambling*** and ***financial services***. AUSTRAC considers Crown Melbourne to be a "major reporting entity", alongside CBA, Westpac, STAR and others, which means we are consulted by the regulator with respect to changes impacting the AML/CTF space.

2. **Designated Services**: These designated services provided by Crown Melbourne can be summarised as follows:

   - Placing and receiving bets (e.g. table games, EGMs, ETGs);
   - Connecting people to place bets against each other (e.g. poker);
   - Paying out winnings (Cage);
   - Exchanging cash for chips/tokens, and vice versa (Table, Maple Booth, Tournament Booth, Cage);
   - Accepting the entry of a person into a game (e.g. two-up)[1];
   - Account keeping services (Deposit Account; Card Play Extra; CCF; Credit to O/S); and
   - Foreign exchange services (Cage, hotels).

   Crown Melbourne conducts its designated services in both AUD and HKD.

   The majority of these designated services are delivered on a face-to-face basis.

3. **Other Services:** Crown provides additional services that are not "designated services" for the purposes of the Act (arguably accounts may fall within this due to definitions, however Crown has always taken the view that accounts are to be treated as if they fall within the confines of the Act), but which may otherwise give rise to ML/TF risk. These include, for example:
   - offering safe deposit boxes,
   - gift cards; and
   - crown dollars,

   the latter of which can be bought in cash and redeemed for chips.

[1] Please note that this is subject to further verification.

The risk assessment in respect of these products currently falls under general risk management at Crown Melbourne. A different approach has been taken historically at Crown Perth, with certain of these services falling within the Crown Perth AML/CTF Program.

4. **Who are our customers?** Crown Melbourne has a variety of persons to whom it provides designated services, including a number that are gmabling for entertainment and may not be identified. These persons could include:

- **General patrons**: individuals that may or may not be provided with a designated service, but are otherwise at Crown's facilities for the purposes of entertainment (bowling, arcade, cinemas, bars, restaurants, shopping). **These patrons are not directly assessed for their ML/TF risk, with any risk presented by these patrons ultimately reviewed under Crown Melbourne's risk management policy and processes.**

- **Main gaming floor punters**: these are individuals that may be provided a designated service (e.g. play an EGM) and, as they sit under the $10,000 cash threshold in the AML/CTF Rules, are not identified by Crown Melbourne (unless they are a Crown Rewards customer). These punters may be out for a once in a period visit, or may be regular customers. The latter may be Crown Rewards customers (see below).

- **Crown Rewards Customers**: where a customer has signed up to be a Crown Rewards customer, he or she will be identified by Crown in accordance with the AML/CTF Act, notwithstanding Crown may not be required to do so (due to exceptions in the Act applicable to casinos).

- **Threshold transaction customers**: where a customer conducts a cash transaction of $10,000 or more, Crown Melbourne will take ID and will lodge a threshold transaction report in accordance with the AML/CTF Act.

- **Casino management account customers | CCF | Foreign Credit**: where Crown Melbourne provides an account facility to a customer, that person will be identified at the time of opening the account, and at each occasion when transacting on the account. The exception is Cashless (Card Play Extra), where a PIN is provided to a customer in order for that customer to use the Cashless functionality. A number of customers provided with credit will be subject to enhanced customer due diligence, including obtaining C6 and other source of funds / source of wealth information reports.

- **VIP Customers**: where a customer is a VIP Customer, he or she will be identified by Crown. In order to enter a VIP room, a customer must "swipe in" to a MICK machine at the door. Compliance with the identification requirement of customers and their guests is reviewed regularly by the Compliance Audit department.

  VIP Customers may be domestic or international, may be playing on a Program (specific to a particular method of delivery of a designated service – for example, an EGM program).

- **Junket Operators**: all junket operators are considered and approved, with ECDD and ID taken.

- **Key Players under Junkets**: all key players will provide two forms of appropriate identification to Crown.

5. **AML/CTF Program**. Crown Melbourne has an AML/CTF Program in place which has been reviewed by both the regulator, Ernst & Young (in 2010) and by our internal audit team (the latter on an independent basis). This AML/CTF Program is based off a pro forma developed by the (now defunct) Australian Casinos Association at or about 2006-7 upon the introduction of the AML/CTF Act and Rules. **A Regulatory Road Map is currently under compilation and will be provided upon completion.**

6. **Review of existing designated services**: Risk identification, mitigation and management of existing designated services is conducted under the AML/CTF Program on an annual basis (at a minimum).

   From information viewed, this has been conducted historically by the Legal Team at Crown Melbourne, with input from the AML/CTF Committee. Unfortunately, due to staff changeover it has been difficult to locate the detail of these reviews to date in a fulsome manner. I do note, however, the risk annexure to the AML/CTF Program refers to EY and other confirmations that I have been advised (by Sasha Grist) are more than 12 years old. Particular risks identified by the business (for instance, risks included in the AUSTRAC Guidelines document) are not on the register. **There are opportunities to enhance the existing document to ensure it is current and reflects the breadth of the risk reviews conducted.**

   To that end, this year's annual review in March / April has actively engaged the business, with the view to updating the 'controls' section to ensure it reflects the various controls already ingrained in the business.

   This review process includes a consideration of potential vulnerabilities and appropriate controls to address those vulnerabilities. This has included an assessment of Crown's susceptibility to crime, and how that is mitigated by the solid relationship between Crown and the Victorian and Federal Police.

7. **Review of proposed new designated services, or changes in methods of delivery, tech etc**: Risk identification, mitigation and management of proposed designated services are conducted by way of an Approval Form. This Approval Form is completed by the business, reviewed by the GGM-AML, considered by the AML/CTF Committee and signed off by the AML/CTF Compliance Officer as he sees fit.

8. **AML/CTF Risk Awareness Training**: Crown Melbourne presently trains its 'relevant staff' as follows:

   - Upon induction;
   - Every second year (**Refresher Training**);
   - On an ad hoc basis (for example, when a new designated service is released – the most recent example being the chip dispensing machine); and
   - On a remedial basis.

   Following my commencement, and following feedback from AUSTRAC as to how important training is (which has been acknowledged by Crown Melbourne, particularly given the transaction monitoring that occurs on a live basis by staff) – Crown Melbourne has implemented a concerted campaign to ensure all outstanding staff have completed Refresher Training.

   As a result of that effort, in particular by Matthew Christie, the business compliance rate now sits at above 90%, with an upward trajectory.

The responsibility of ensuring that AML/CTF Training is completed falls to the CTRM. On current resourcing, the CTRM does not have the present capacity to ensure that individual employees complete their training – this has been handed to me. Please see my observation below – this should be handled by HR who has close access to the training, and the Senior Executive team so they have oversight of each of their respective departments. This is not a large departure from existing process.

The AML/CTF Risk Awareness Training is due a refresh. **This is presently under review.**

9. **Employee Due Diligence**: Crown Melbourne screens all prospective employees as required by the VCGLR (including, for example, a credit check or police check as required). The AML/CTF Program identifies that this screening is an appropriate risk based system for Crown Melbourne to determine whether an employee might be in a position to facilitate the commission of a money laundering or terrorist financing offence in the connection of providing a designated service.

   This rationale should be documented as a verification piece for the Joint Program.

10. **Customer Identification:** As referenced at 4 above, customer identification is undertaken in compliance with the AML/CTF Act and Rules by a number of different business units, specifically:

    - **EGMS**: by the Crown Rewards team at the Crown Rewards booth, or by customer service attendant if the customer conducts a transaction of a certain magnitude (e.g. collect of $20k or more on an EGM on the MGF or $75k or more in a VIP room);

    - **Table Games**: at the table, at the Maple Booth, at any Tournament Registration Booth;

    - **Cage**; and

    - **Floor**: on the floor from time to time (for example, signing up a customer for a Crown Rewards Card).

    I have been made aware of some errors in respect of Appropriate ID by Compliance Audit (staff members inputting incorrect expiry dates on IDs – establishing accounts with expired ID). I have raised with Compliance Audit that we should include as a query in their audit what remedial training is provided to these staff members, and if it hasn't been provided, why not. This was relayed in the AML/CTF Committee meeting on 30 April 2018 to Kierren Gersbach.

11. For the purposes of AML/CTF Act and Rules compliance (except as otherwise noted below), customer identification is taken:

    - For transactions of $10,000 in cash or more at the Cage, at a Table, or at a Booth;
    - Upon setting up a Crown Rewards account (not an AML/CTF Act requirement but a requirement under the Crown Rewards T&C);
    - When establishing Card Play Extra (the facility of depositing and withdrawing cash on the Crown Rewards Card);
    - When establishing a cheque cashing facility (**CCF**);

- When establishing a Deposit Account;
- When conducting foreign exchange transactions of $1,000 cash or more;
- When withdrawing or depositing funds to a Deposit Account (at the Cage); and/or
- If a suspicion arises, although the extent to which information is obtained in this situation is unclear and dependent upon whether such information is available to Crown Melbourne (keeping in mind the prohibition against tipping off a customer).

12. **Transaction Monitoring**: Crown Melbourne conducts a number of different forms of monitoring as follows:

- On a live basis in the provision of designated services (for example, by a dealer or by a cashier). This is referred to in the AML/CTF Program as "observational", and is Crown's strength. It is also why it is critical that we continue to push for as close to 100% attendance on AML/CTF Risk Awareness Training as we possibly can.
- By the Cash Transactions Reporting Manager (**CTRM**), or his designee Sean Counihan, where work permits. Sean Counihan is a compliance manager and reports to the Group General Manager – Regulatory and Compliance.
- By the Group General Manager – AML, in respect of certain identified activity to assess potential ML/TF risk (for example: "*the life of a TITO*").

Crown Melbourne does not have automated transaction monitoring of its designated services in the way a financial services institution does (for example). **This is an area of opportunity for the business, particularly as it provides designated services to patrons who may not otherwise be identified by Crown.**

For instance, other than observational monitoring (which is limited), Crown Melbourne does not presently have any monitoring of:

[redacted]

13. The current 'transaction monitoring' undertaken by the CTRM (and some comments) listed in the AML/CTF Program can be summarised as follows:

- **Threshold Transaction Reports**. This is largely quality assurance work, as distinct from transaction monitoring. The quality assurance piece is important to ensure that the information we lodge with AUSTRAC is correct (as has been made patently clear with respect to our recent IFTI issues).

- **Buy-In Report**. All transactions of $10,000 or more. Given these transactions will be caught by TTRs lodged (as any buy-in of more than $10,000 in cash requires a TTR). **This report has been flagged to remove from transaction monitoring.**

- **Alert Report**. This is a valuable report that enables the CTRM to monitor a particular customer's transactions where they have engaged in otherwise unusual activity. This is KYC (and perhaps ECDD), and potentially transaction monitoring.

- **Multiple cheques**. Crown Melbourne has identified that this includes cheques over $5,000, but has not formed a view on how many cheques might constitute "suspicious" behaviour for a customer, so views them all. **Query the utility in this given limitations on resources. As part of**

the Joint Program, to assess the number of cheques and, applying a risk based approach, consider what constitutes suspicious behaviour (for example, is it 6 cheques in 3 months?)

- **Multiple buy-ins accumulative totalling $9,000 per day**. This is to identify potential structuring activity. This is valuable and is transaction monitoring. One day a week.

- **Bankruptcy Report**. **This is "know your customer", not transaction monitoring.**

- **Cancel Credits / Jackpot Report**. This involves reviewing cancel credits/jackpots during the day. This is an important report, as there have been instances where customers have claimed bill stuffing as jackpot wins in the past (directly addressing an ML/TF Risk). This report however is a manual report that has contained errors out of the EGMs team. The EGMs team presently has the pen on whether we can automatically generate a report out of CDW to remove the capacity for human error.

- **Occupation**: **This is "know your customer", not transaction monitoring.**

- **Foreign Currency Exchange**: reviews conducted by Compliance on a regular basis. This is transaction monitoring. GGM-AML reviews monthly transactions at Hotels to look for unusual activity.

- **TTs**: the CTRM checks telegraphic transfers into, and out of, customer accounts. This is on a line-by-line basis, without any tools to assist him and is a laborious process.

- **Direct Transfers**: Crown Melbourne customers can transfer deposited funds between themselves through a "direct". These transfers are reviewed on a manual basis.

- **Junket Program**: the CTRM reviews the transactional activity of all key players of a junket of $50,000 or more upon settlement of a program. This is a laborious task, and I have had initial discussions with the CTRM as to whether he can identify what he looks for, so that analysis might form part of the likely same process occurring in VIP Finance.

14. In addition to the above, VIP Finance will monitor the gaming behaviour of certain of identified key players and VIP customers, including the turnover of particular Chinese patrons.

15. The reports utilised in the Transaction Monitoring Program above effectively act as follows:
    - A customer's name will appear on a report.
    - The CTRM will then look at the customer's activity.

The intention of putting in place a Transaction Monitoring Programs is to have the purpose of identifying, having regard to ML/TF Risk, any transaction that appears to be suspicious within the terms of section 41 of the AML/CTF Act. In addition, it should have regard to complex, unusual large transactions and unusual patterns of transactions, which have no apparent economic or visible lawful purpose.

To this end, Crown has some opportunities to enhance its existing framework. Please see the comments in Observations.

16. **Assessment of Customer Risk**: The assessment of risk on customers is assessed by the CTRM (or his delegate). Customer Risk profiles are retained by the CTRM in his email (C Drive). The position taken under the AML/CTF Program is that all customers are of low risk until evidence is presented otherwise (this differs to Perth).

    An SOP is currently under development for the CTRM that will address improvements to this process, including pre-preparing for the CURA roll-out later this year.

    The current Customer Risk Assessment can be improved by some improvements as to process. I note that the CTRM reports changes to risk profile at a high level to the AML/CTF Committee.

17. **Customer Risk Assessment by VIP Finance**: It is arguable that customer risk assessment is also conducted by VIP Finance (Mary Gioras and her team), although the extent to which this information is shared with the CTRM is limited (albeit improving). Mary Gioras conducts daily reviews of particular customers from China as noted above.

    There are opportunities to address structure and move this work under AML, or in the alternative, at least capture this work in the customer ML/TF risk assessment. There is presently duplication here.

18. Where a customer is determined to present a high ML/TF risk to Crown Melbourne, or otherwise as required under the Act (for instance, foreign PEPs, where an SMR is to be filed), Crown Melbourne has historically taken the following steps to conduct enhanced customer due diligence:

    (a) Checking the patron's SYCO account for transactional history;
    (b) Clarifying or updating KYC information already collected on a customer; and
    (c) Obtaining senior management approval.

    An observation as to ECDD is included below.

    There is a real opportunity to enhance the communication of where ML/TF risk is identified by the CTRM. That is, that the relevant senior executives in relevant teams are aware of this assessment. It is not clear whether is presently the case and this requires further analysis.

19. **Reporting Obligations**. Crown Melbourne must lodge reports including in respect of threshold transactions ($10k cash+), international funds transfer instructions (gaming) and suspicious matters. The process for lodging these forms is as follows:

(a) Threshold transaction reports are prepared by TG or the Cage, and are sent to the CTRM to check and lodge. TTRs must be lodged within 10 Business Days from the transaction date.
(b) International Funds Transfer Instructions are prepared by the Cage and are lodged by VIP Finance. IFTIs must be lodged within 10 Business Days from the transaction date. **We have had another issue here, as recently as 26 April the team indicating they didn't know what they had to check or why. This is being resolved with Mary Gioras and her team.**

(c) Suspicious Matter Reports are prepared by the relevant individual identifying the suspicion and forwarded to the CTRM to consider, add value and lodge. Crown Melbourne has taken the view that the AML team as a general rule lodges all SMRs forwarded to him. In this way, the CTRM acts as a post-box. **This is not necessarily the wrong approach, but there is an opportunity here to enhance the program, including by making sure that the CTRM categorises the nature of the suspicion so the team can drill down as to whether the ML/TF risk register (or customer register) needs to be reviewed.**

An observation on the efficiency and level of assurance on reporting is provided at Observations below, as well as identifying some ways we can now enhance the reporting of SMRs (internally) as a result of my appointment, and pending the finalising of the SOP.

20. **Compliance Team:** The Crown Melbourne direct AML team is comprised as follows:

(a) The AML/CTF Compliance Officer (the CLO);
(b) The Group General Manager – AML [New]; and
(c) The CTRM.

The team is supported by compliance champions across the business and the compliance function where needs arise and bandwidth is available. The level of support when it is available is excellent, with a good breadth of experience. However, please see my comment as to training.

The team is also supported by VIP Finance as it relates to ECDD and IFTI reporting. **There is a level of overlap here that could lead to potential savings or reallocation of resources to drive efficiencies.**

There is clearly some duplication of roles, entirely expected given the growth of AML through the business and the way things have been operated to date. There is an excellent opportunity to streamline the team, and potentially better allocate resources. Some recommendations on staffing is provided in this Report.