STATEMENT OF NEIL GEORGE JEANS – RFS – Initialism - 001

ANNEX B

CROWN RESORTS

Transaction/Activity Monitoring Review

Q4 2018 and Q1 2019

INITIALISM
AML compliance solutions

Background

Crown Melbourne Limited (**Crown Melbourne**) and Burswood Nominees Limited (ATF the Burswood Property Trust) (**Crown Perth**) (collectively, **Crown**) requested Initialism conduct an independent review of their transaction monitoring programs, which forms part of its AML/CTF Programs.

Crown has two (2) reporting entities across two sites, Crown Melbourne and Crown Perth.

The purpose of the review is to assess Crown's monitoring of customer activity undertaken to comply with its on-going customer due diligence obligations and identify any opportunities to adjust, refine and where appropriate enhance Crown's monitoring.

Scope

Initialism conducted the review through:

- Reviewing the documented monitoring approach and processes for monitoring customer and gaming transactional activity as part of the AML/CTF Programs of Crown Melbourne and Crown Perth and supporting documented policies and procedures, including testing assumptions based upon the underlying assessment of ML/TF risk.

- On-site testing and sampling in Crown Melbourne of actual examples of Crown's day to day operations to assess the effectiveness of the monitoring of activity to identify unusual behaviour.

- The identification of opportunities to refine and adjust activity monitoring, through on-site workshops and compliance and business engagement, where necessary.

- Providing a written report outlining findings, recommendations, and options for refinement where necessary.

Limitations

Initialism carried out its review on a test basis. The review, in practice, cannot examine every activity and procedure, nor can it be a substitute for management's responsibility to maintain adequate control of all levels of operations, and their responsibility to prevent and detect irregularities.

Executive Summary
Findings

Based upon the work undertaken, Crown is meeting is obligations under section 36 of the AML/CTF Act, as it is monitoring customers using designated services to identify, mitigate and manage the risk of a customer's use of a designated service being involved in or facilitating money laundering or terrorist financing.

Based upon the work, Crown is meeting the requirements of Chapter 15 of the AML/CTF Rules, as the monitoring undertaken is documented in the AML/CTF Programs, and includes appropriate systems and controls to undertake the monitoring to facilitate the identification of suspicious matters, and seeks to identify complex, unusually large transactions and patterns of transactions which have no apparent economic or visible lawful purpose.

Crown has appropriately focused the monitoring controls within its Transaction Monitoring Programs (**TMP**) on the use of Casino Value Instruments, including chips, tokens, gaming tickets, cheques and other instruments (**CVIs**), gaming accounts and designated services. Crown's TMPs leverage a series of reports from business systems, these reports cover the activity and use of all relevant CVIs, gaming accounts and services designated by the AML/CTF Act.

Crown's monitoring across both Crown Perth and Crown Melbourne is manual, largely relying on the manual review by the AML Team and/or, where relevant, the Business Units, of system-generated reports to identify triggers in customer activity. The customer that is the subject of the trigger's activity is then subsequently manually reviewed through an analysis of business systems to assess activity.

The manual review to identify suspicious activity based upon identified triggers is also based upon and heavily reliant upon the reviewer's experience and knowledge, and is standardised and consistent on an entity but not enterprise level. The current monitoring is time consuming and means skilled resources are undertaking activity that could be automated/systemised, which impacts the potential scalability of the current approach.

The recording of monitoring activity and outcomes is systematic for Crown Melbourne and Crown Perth but not as yet at the enterprise level. This means there is currently no expedient way to search previous monitoring activity to identify trends or patterns, as triggers and recording of customer information is siloed to each location and not possible across the enterprise.

Crown Perth have a more systematic approach to recording the outcomes of the TMP, as the outcomes of the manual review to identify triggers and the subsequent analysis and decisioning are recorded and retained within a separate risk register. This recording of monitoring activity and outcomes in a more systematic way means there is a systematic way to search previous monitoring activity to identify trends or patterns not detected by triggers.

Initialism's review identified a number of variations between the two monitoring regimes, which appear to be driven by different gaming practices and regulation, as well as historic processes at both properties.

The reports used by Crown to identify triggers contain a significant number of data points/elements which could be leveraged to refine the monitoring and systemise the manual trigger review process. Initialism as part of its review made recommendations to refine and leverage key data elements contained within the current reports.

During the review Initialism were informed of significant developments to TMP which have been developed by Crown's AML Team and are due to be rolled out.

Initialism reviewed a UAT version of the revised systematic monitoring and it appears that the automation will be at least equivalent to the current manual trigger identification and will provide increased sustainability and scalability to Crown's monitoring activity.

Recommendations

Whilst it is noted that Crown appears to be complying with its obligations under the AML/CTF Act and Rules, as a result of the review Initialism make the following recommendations to refine and enhance current monitoring.

It is noted that Crown has already embarked on a new technology framework for TMP which will address many of the recommendations below and improve the sustainability and scalability of Crown's TMP, and support continuously improvement of the already compliant Crown TMP.

Current TMP Activity

Crown's current monitoring is manual. Automating the trigger identification as much as possible, will free up skilled resources within the AML Team to do more value-add work.

Crown Perth and Crown Melbourne both rely on a number of business operations as well as the AML Team to undertake TMP activity and consideration should be given to ensure that TMP activity is undertaken by the most appropriate function to minimise duplication and increase efficiency.

Crown Melbourne should revise its TMP record keeping from the current manual and fragmented process and consider adopting the risk register centralised recording process currently used by Perth or develop a standardise approach across the enterprise.

Crown Perth should consider introducing Aged TITO monitoring, to ensure monitoring is as consistent as possible across Crown Melbourne and Crown Perth.

Proposed Automation

The introduction of the automation of trigger identification is an important enhancement for Crown, as the current manual processes are potentially not sustainable and scalable with current resources should Crown's business footprint expand, or Crown offers further designated services and/or introduces new delivery methods.

As Crown introduces the automation, whilst it appears that the proposed automation will provide an equivalent level of monitoring to current activity, it will be important for Crown to ensure that the automation does not degrade current monitoring levels and to establish a review and refinement process to adjust thresholds and scenarios/rules within the automation should circumstances dictate.

Crown should also establish a periodic review process as part of its TMP to ensure the scenarios/rules remain appropriate.

Obligations to monitor customers

As a reporting entity under the AML/CTF Act 2006, Crown has obligations to monitor its customers in order to identify unusual and possibly suspicious activity, which may require reporting under the requirements of section 41 of the AML/CTF Act. Crown's obligations to monitor are set out in both the AML/CTF Act and Rules. Section 36 of the AML/CTF Act states that:

> *(1) A reporting entity must:*
>> *(a) monitor the reporting entity's customers in relation to the provision by the reporting entity of designated services at or through a permanent establishment of the reporting entity in Australia, with a view to:*
>>> *(i) identifying; and*
>>> *(ii) mitigating; and*
>>> *(iii) managing;*
>> *the risk the reporting entity may reasonably face that the provision by the reporting entity of a designated service at or through a permanent establishment of the reporting entity in Australia might (whether inadvertently or otherwise) involve or facilitate:*
>>> *(iv) money laundering; or*
>>> *(v) financing of terrorism; and*
>> *(b) do so in accordance with the AML/CTF Rules.*

This establishes the obligation to monitor customers using designated services to identify, mitigate and manage the risk that a customer's use of a designated service involves, or is facilitating, money laundering or terrorist financing.

The Act also requires reporting entities to comply with the monitoring requirements set out in the AML/CTF Rules. Chapter 15 of the AML/CTF Rules, states:

> *Transaction monitoring program*
> - *15.4 A reporting entity must include a transaction monitoring program in Part A of its AML/CTF program.*
> - *15.5 The transaction monitoring program must include appropriate risk-based systems and controls to monitor the transactions of customers.*
> - *15.6 The transaction monitoring program must 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.*
> - *15.7 The transaction monitoring program should have regard to complex, unusual large transactions and unusual patterns of transactions, which have no apparent economic or visible lawful purpose.*

The Rules define the scope of the transaction monitoring program. The Rules establish that it should be documented in the AML/CTF Program and include appropriate systems and controls to undertake the monitoring to facilitate the identification of suspicious matters, and identify complex, unusually large transactions and patterns of transaction which have no apparent economic or visible lawful purpose.

Initialism have used the legal and regulatory requirements set out by the AML/CTF Act and Rules as part of the basis for the review of Crown's TMPs.

Review

Initialism reviewed the adequacy of the transaction monitoring currently being undertaken by Crown.

The review included an assessment of Crown's TMPs as documented in its AML/CTF Programs, and an assessment and analysis of Crown's existing processes and activity, as well as meetings with relevant stakeholders and AML Team members, including the Group General Manager AML.

The work undertaken as part of the review resulted in the following findings:

Findings

Crown offers a number of services designated under the AML/CTF Act. All designated services are, by definition, vulnerable to being used and abused by criminals engaged in criminal conduct and/or to launder the proceeds of criminal conduct.

Crown Melbourne and Crown Perth TMPs are set out in the AML/CTF Programs (and for Crown Perth, it is further articulated in the AML Officer's Standard Operating Procedures), and covers all the designated services offered by Crown.

As part of the AML/CTF Programs (Appendix 1), Crown has also assessed the risk of each designated service, documenting how each designated service could be used to facilitate ML/TF, and then documenting the specific controls in place to manage and mitigate the risk. The controls specified in Appendix 1 include the transaction monitoring activity undertaken by Crown at Crown Melbourne and Crown Perth.

The AML/CTF Programs therefore directly align the risk or vulnerability of each designated service offered by Crown to being used to facilitate ML/TF to the transaction monitoring activity being undertaken.

Based upon Initialism's review, Crown is to be meeting its obligations under section 36 of the AML/CTF Act, as it is monitoring customers using designated services to identify, mitigate and manage the risk of a customer's use of a designated service being involved in or is facilitating money laundering or terrorist financing.

Crown also is to be meeting the requirements of Chapter 15 of the AML/CTF Rules, as the monitoring undertaken is documented in the AML/CTF Programs, includes appropriate systems and controls to undertake the monitoring to facilitate the identification of suspicious matters, and seeks to identify complex, unusually large transactions and patterns of transactions which have no apparent economic or visible lawful purpose.

Crown's ML/TF risk assessment of its business operations in both Crown Melbourne and Crown Perth appropriately establishes that its ML/TF vulnerabilities are focused on the receipt and payment of funds and conversion of value into Casino Value Instruments[1] (CVI) and the transfer of value between CVIs.

Crown have appropriately focused the monitoring controls on transactions and the use of CVIs and designated services. Crown services utilise the following CVIs – Cash / Casino Chips / Ticket In Ticket Out (TITO) / Casino Cheques.

---

[1] FATF Casino's Typology Report 2009 - Casinos utilise various value instruments to facilitate gambling by their customers. Casino value instruments are most often used for money laundering by converting illicit funds from one form to another.

Current TMP Activity

Crown's TMP in both Melbourne and Perth leverages a series of reports from business systems, these reports cover the activity and use of all relevant CVIs and designated services (table 3, section 6, AML/CTF Act).

The reports utilised are:

Report	Casino Value Instrument (CVI)
Cash Transactions Report for transactions of A10,000 (or its equivalent) or more	Chips, CPVs, Ticket In Ticket Out (TITO) Tickets (also known as Gaming Tickets), Casino Cheques.
Gaming Cheque Report	Casino Cheques
Buy-ins Reports	Chips
EGM / ETG Activity Report*	TITO Tickets
Cancel Credits and Jackpots Report (EGM/ETG)*	Cash, Casino Cheque, TITO Tickets.
TITO Tickets Report*	TITO Tickets.
Foreign Currency Transactions Report	N/A (review of transactions)
Higher Risk Customer Activity Report (SYCO Alerts Report)	N/A (review of transactions)
Direct Transfer Report	N/A (review of transactions)
Telegraphic Transfers Report	N/A (review of transactions)
Bankrupt Report	N/A
Junket Program Report	N/A
Security Daily Report*	Events and Behaviour of Patrons (including use of designated services)
Surveillance Report*	Events and Behaviour of Patrons (including use of designated services)
Fusion Gaming Machine Report^	Cash; TITO Tickets.

Report	Casino Value Instrument (CVI)
iTrak Report^	Events and Behaviour of Patrons (including use of designated services)
Note: Those marked with * are reviewed by Crown Melbourne only and those marked ^ are reviewed by Crown Perth only	

The way these reports are used and who undertakes the monitoring activity (business operations or the AML Team) varies between Melbourne and Perth. Initialism have analysed the TMPs in both Melbourne and Perth.

Crown Melbourne

Each of Crown Melbourne's current transaction monitoring activities covers one or more CVIs. The following is a table of Crown Melbourne's current monitoring activity:

Activity/attribute monitored	Method	CVIs/DS/Other Covered	Frequency of Report	Rationale/Criteria	Process followed	Recording of outcomes
Live monitoring of customer behaviors	Staff Observation reported via Floor Reports.	Live monitoring looks at all behaviour. It could be with respect to a CVI; the use of a designated service; other behaviour.	As Observed	Unusual behavior observed by staff which may be indicative of suspicious activity.	Manual review of reported activity against SYCO and other Crown databases to determine if suspicious.	Recorded in SYCO under Patron record and manual records retained by AML Team. Where an SMR is filed, a record is retained against the Customer's Crown number in Crown's SEER database, with a record of the SMR retained by the AML Team.
Cash transactions of A$10,000 (or its equivalent) or more	Report from SYCO of relevant transactions – Cash Transaction Report	Chips, CPVs, Ticket In Ticket Out (TITO) Tickets (also known as **Gaming Tickets**), Casino Cheques	Daily	Review of TTRs (A$10,000+) to identify usual patterns of behavior.	Manual review by AML Team of transactions in the Report to identify triggers and then manual analysis of triggered activity against SYCO (or other Crown systems) to identify anything suspicious.	Recorded in SYCO under Patron record and manual records retained by AML Team. Where an SMR is filed, a record is retained against the Customer's Crown number in Crown's SEER database, with a record of the SMR retained by the AML Team.

Activity/attribute monitored	Method	CVIs/DS/Other Covered	Frequency of Report	Rationale/Criteria	Process followed	Recording of outcomes
Cheques of A$5,000 or more issued to patrons and customers	Report from SYCO of relevant transactions – Cheque Report	Cheques	Daily	Review of cheque issuing over a A$5,000 threshold to identify potential unusual patterns of behavior based on overall activity of patron.	Manual review by AML Team of transactions in the Report to identify triggers and then manual analysis of triggered against SYCO (or other Crown systems) to identify anything suspicious.	Recorded in SYCO under Patron record and manual records retained by AML Team.\n\nWhere an SMR is filed, a record is retained against the Customer's Crown number in Crown's SEER database, with a record of the SMR retained by the AML Team.
Single buy-ins at a gaming table of A$10,000 (or its equivalent) or more	Report from SYCO of relevant transactions – Buy-in Report	Chips, Cash	Daily	Review purchases of chips of A$10,000 (or its equivalent) or more away from the 'cage' facilities to identify potential unusual patterns of behavior based on overall activity of patron.	Manual review by AML Team of transactions in the Report to identify triggers and then manual analysis of triggered activity against SYCO (or other Crown systems) to identify anything suspicious.	Recorded in SYCO under Patron record and manual records retained by AML Team.\n\nWhere an SMR is filed, a record is retained against the Customer's Crown number in Crown's SEER database, with a record of the SMR retained by the AML Team.
Multiple buy-ins by a customer that total A$9,000 (or its equivalent) or more in a single	Report from SYCO of relevant transactions – Buy-in Report	Chips, Cash	Weekly (One day randomly selected from the	Review of multiple smaller purchases of chips away from the 'cage' facilities that total over an A$9,000	Manual review by AML Team of transactions in the Report to identify triggers and then manual	Recorded in SYCO under Patron record and manual records retained by AML Team.\n\nWhere an SMR is filed, a record is retained against the

Activity/attribute monitored	Method	CVIs/DS/Other Covered	Frequency of Report	Rationale/Criteria	Process followed	Recording of outcomes
day for Table Games			previous week)	threshold to identify usual patterns of behavior based on overall activity of patron.	analysis of triggered activity against SYCO (or other Crown systems) to identify anything suspicious.	Customer's Crown number in Crown's SEER database, with a record of the SMR retained by the AML Team.
TITO Tickets with a value of more than A$5,000 aged more than 24 hours	Report from DACOM – TITO Ticket Report	TITO Tickets	Weekly	Review of EGM and ETG produced TITO Tickets valued over a threshold that have not been redeemed within 24 hours to identify unusual patterns of behavior.	Manual review by AML Team of transactions in the Report to identify triggers and then manual analysis of triggered activity against SYCO to identify anything suspicious.	Recorded in SYCO under Patron record and manual records retained by AML Team.
Chip Dispensing Machine activity	Report from SYCO	Cash, Chips	Monthly	Review of activity through the Chip Dispensing Machine to identify unusual patterns and possible structuring (transaction cap of A$2000 per transaction).	Manual review by AML Team of transactions in the Report to identify anything suspicious.	Recorded in SYCO under Patron record and manual records retained by AML Team.
Activity on EGMs and ETGs over a gaming day	Report from Data Warehouse –	TITO Tickets	Daily	Review of activity through a particular	Manual review by AML Team of machine usage	Recorded in SYCO under Patron record (if Patron known) and

Activity/attribute monitored	Method	CVIs/DS/Other Covered	Frequency of Report	Rationale/Criteria	Process followed	Recording of outcomes
	EGM/ETG Report			EGM/ETG to identify potential unusual usage/activity through a particular machine.	and type of activity in the Report to identify triggers and then manual analysis of related activity in SYCO or other Crown systems (e.g. DACOM) to identify anything suspicious.	manual records retained by AML Team.
Cancel credits and jackpots on EGMs and ETGs by a single customer	Report from SYCO or other Crown databases of relevant transactions – Cancel Credit and Jackpot Report	TITO Tickets, Cash, Cheques	Daily	Review of customers that request the withdrawal account held funds to identify unusual patterns of behavior.	Manual review by AML Team of transactions in the Report to identify triggers and then manual analysis of triggered activity against SYCO to identify anything suspicious.	Recorded in SYCO under Patron record and manual records retained by AML Team.
Foreign currency transactions by a customer across the Crown estate	Report from SYCO of relevant transactions - Foreign Currency Transactions Report	Cash	Ad-Hoc	Review of FX transactions by customers over a A$1,000 (or foreign currency equivalent) threshold to identify usual	Manual review by AML Team of FX transactions in the Report to identify triggers and then manual analysis of triggered activity against SYCO or	Recorded in SYCO under Patron record and manual records retained by AML Team.

Activity/attribute monitored	Method	CVIs/DS/Other Covered	Frequency of Report	Rationale/Criteria	Process followed	Recording of outcomes
				patterns of behavior.	other Crown systems (e.g. Opera) to identify anything suspicious.	
Higher risk customer activity monitoring	Report from SYCO of relevant transactions by specified customers risk rated 'significant' or 'high' risk - Higher Risk Customer Activity Report	All	Daily	Review of activity and use of facilities by specific designated patrons across the Crown complex to identify unusual patterns of activity.	Manual review by AML Team of a designated patron's activity in the Report to identify triggers and then manual analysis of patrons with trigger activity against SYCO to identify anything suspicious.	Recorded in SYCO under Patron record and manual records retained by AML Team.
Direct Transfer between customer accounts	Report from SYCO - Direct Transfer Report.	Account Activity	Ad-hoc	Review of patron to patron transfers to identify unusual patterns of activity.	Manual review of a designated patron's activity in the Report to identify triggers and manual analysis against SYCO to identify	Recorded in SYCO under Patron record and manual records retained by AML Team.

Activity/attribute monitored	Method	CVIs/DS/Other Covered	Frequency of Report	Rationale/Criteria	Process followed	Recording of outcomes
					anything suspicious.	
Screening the names of customers	Data matching between SYCO Data and Screening provider.	Account Activity / Crown Rewards and other Crown assigned number to the Customer (e.g. VIP). The latter is not a designated service nor a CVI.	Daily	Review of results of screening customer names against PEP and SDN lists.	Manual review of alerts generated by Dow Jones system.	Recorded in SYCO under Patron record and records retained by AML Team (Dow Jones).
Telegraphic Transfers	Report from SYCO	Account Activity	Daily	Review of Telegraphic Transfers undertaken for customers to identify unusual patterns of activity.	Manual review of a designated patron's activity in the Report to identify triggers and manual analysis against SYCO to identify anything suspicious.	Recorded in SYCO under Patron record and manual records retained by AML Team.
Surveillance Identified Activity	Notification from Surveillance Team	All	Ad-Hoc	Review of all AML/CTF matters identified by Surveillance Team activity.	Manual analysis of surveillance footage and SYCO to identify	Manual records retained by AML Team.

Activity/attribute monitored	Method	CVIs/DS/Other Covered	Frequency of Report	Rationale/Criteria	Process followed	Recording of outcomes
					anything suspicious.	
Security Identified Activity	Operations Report	All	Daily	Review of report to identify AML/CTF activity.	Manual analysis of Operations Report to identify anything suspicious.	Manual records retained by AML Team.
Notices of persons becoming bankrupt	Data matching	N/A	Ad-Hoc	Review of activity of patrons that are subject to bankruptcy orders.	Manual review of patrons listed in the Report to identify triggers and analysis against SYCO activity to identify anything suspicious.	Recorded in SYCO under Patron record and manual records retained by AML Team.
Gaming Trends	Report from SYCO	All	Annually	Review of patterns of activity by patrons to assess level of activity against previous activity to identify unusual levels of activity.	Manual review of a patron's activity (T/O, Win Rate, Number of Visits) to identify triggers manual analysis against SYCO to identify anything suspicious.	Recorded in SYCO under Patron record and manual records retained by AML Team.

Activity/attribute monitored	Method	CVIs/DS/Other Covered	Frequency of Report	Rationale/Criteria	Process followed	Recording of outcomes
Centrelink concession cardholder (to the extent known)	Data matching	N/A	Annually	Review of patterns of activity by patrons with Centrelink status to identify unusual levels of activity.	Manual review of a patron's activity and manual analysis against SYCO to identify anything suspicious.	Recorded in SYCO under Patron record and manual records retained by AML Team.
Key Player Report	Report from Data Warehouse	Customer behaviour when using designated services	Ad-Hoc	Review of Junket Players activity to identify unusual patterns of activity.	Manual analysis of player by player activity against SYCO to identify anything suspicious.	Recorded in SYCO under Patron record and manual records retained by AML Team.
Customer Occupation	Report from SYCO	Casino Rewards Cards / Cash / TITO / Casino Chips / Casino Cheques	Ad-Hoc	Review of customers that have been identified as having a higher risk to identify unusual patterns of activity.	Manual review of patrons with specific occupations (bank employees, accountants, lawyers, public servants, tax agents, stockbrokers, PEPs or in other occupations involving the management of a third party's funds) and manual analysis against SYCO to	

Activity/attribute monitored	Method	CVIs/DS/Other Covered	Frequency of Report	Rationale/Criteria	Process followed	Recording of outcomes
					identify anything suspicious.	

Crown Melbourne appears to have a comprehensive transaction monitoring program that monitors the use of CVIs and designated services in a way appropriate to the ML/TF risks faced and to identify complex, unusually large transactions and patterns of transactions which have no apparent economic or visible lawful purpose.

Whilst Crown Melbourne monitoring is manual, as the subject of the trigger's activity is then subsequently manually reviewed through an analysis of business systems to assess activity, the recording of monitoring activity and outcomes is systematic as Crown Melbourne attributes risk ratings to customers in a methodical manner.

The manual review to identify triggers is based and heavily reliant upon the reviewer's experience and knowledge, it is therefore not standardised and consistent at an enterprise level.

The use of manual review at the trigger identification stage of the monitoring process, whilst apparently effective, is also time consuming and means skilled resources are undertaking activity that could be automated/systemised. This would free skilled resources to focus on more value-add type activities in the trigger review.

Crown Perth

As a result of our review of Crown Perth's Standard Operating Procedures[2], the following is a table of Crown Perth's current monitoring activity:

Activity/attribute monitored	Method	CVIs	Frequency	Rationale/Criteria	Process followed	Recording of outcomes
Live monitoring of customer behaviors	Staff Observation reported via Floor Reports.	Live monitoring looks at all behaviour. It could be with respect to a CVI; the use of a designated service; other behaviour.	As Observed	Unusual behavior observed by staff which may be indicative of suspicious activity by patron(s).	Manual review of reported activity against SYCO and other Crown databases and surveillance footage (if available) to determine if suspicious.	Recorded in central (CURA) Patron Risk Register.
Cash transactions of A$10,000 (or its equivalent) or more	Report from SYCO of relevant transactions – Cash Transaction Report and additionally reported in iTrak where the threshold transaction relates to a	Cash	Daily	Review of TTRs (A$10,000+) to identify potential unusual patterns of behavior and/or other suspicious activity.	Manual review by Cage Supervisors at first instance, and the manual analysis of triggered activity is conducted by AML Staff to identify anything suspicious.	Recorded in central (CURA) Risk Register.

---

[2] Legal Services – AML Standard Operating Procedures Version 15 2/11/2018

Activity/attribute monitored	Method	CVIs	Frequency	Rationale/Criteria	Process followed	Recording of outcomes
	Table Games Buy In.					
All cheques issued to customers	Report from SYCO of relevant transactions – Cheque Report	Casino Cheques	Daily	Review of cheque issuing to identify potential unusual patterns of behavior based on overall activity of patron and/or other suspicious activity.	Manual review by Cage Supervisors at first instance, and the manual analysis of triggered activity is conducted by AML Staff to identify anything suspicious.	Recorded in central (CURA) Patron Risk Register.
Single buy-ins at a gaming table of A$10,000 (or its equivalent) or more	Report from SYCO of relevant transactions – Buy-in Report	Cash / Casino Chips	Daily	Review purchases of chips of a A$10,000 (or greater, or its equivalent) threshold away from the 'cage' facilities to identify usual patterns of behavior based on overall activity of patron.	Manual review by Table Games Management of transactions in the Report to identify triggers and then manual analysis of triggered activity against SYCO to identify anything suspicious.	Recorded by Table Games Management on Buy In Reports. Recorded in central (CURA) Patron Risk Register.
Multiple buy-ins by a customer that total A$5,000 or more in a single day	Report from SYCO of relevant transactions	Cash / Casino Chips	Weekly (one day randomly selected from the previous week)	Review of multiple smaller purchases of chips away from the 'cage' facilities that total A$5,000	Manual review by AML Team of transactions in the Report to identify triggers and then	Recorded by Table Games Management on Buy In Reports.

Activity/attribute monitored	Method	CVIs	Frequency	Rationale/Criteria	Process followed	Recording of outcomes
	– Buy-in Report			threshold (or more) to identify usual patterns of behavior based on overall activity of patron.	manual analysis of triggered activity against SYCO to identify anything suspicious.	Recorded in central (CURA) Patron Risk Register.
Activity on ETGs over a gaming day	Report from FUSION	Cash / TITO	Fortnightly	Review of activity through a particular ETG to identify potential unusual usage/activity..	Manual review by Table Games Management of machine usage and type of activity in the Report to detect potential bill stuffing activity or other forms of potential suspicious activity.	Recorded in central (CURA) Parton Risk Register (where patron known).
Foreign currency transactions by a customer across the Crown estate equal to AUD1k or more	Report from SYCO of relevant transactions - Foreign Currency Transactions Report	Cash	Daily	Review of FX transactions by customers over a A$1,000 threshold to identify usual patterns of behavior and/or other suspicious activity.	Manual review by Cage Supervisors of FX transactions in the Report and spot checked by AML Staff, to identify triggers and then manual analysis of triggered activity against SYCO to	Recorded on FEX reports stored at Cage. Recorded in central (CURA) Parton Risk Register where appropriate.

Activity/attribute monitored	Method	CVIs	Frequency	Rationale/Criteria	Process followed	Recording of outcomes
					identify anything suspicious.	
Higher risk customer activity monitoring (SYCO Alert Report)	Report from SYCO or other Crown databases of relevant transactions by specified customers risk rated 'significant' or 'high' risk - Higher Risk Customer Activity Report	Weekly	Daily	Review of activity and use of facilities by specific designated patrons across the Crown complex to identify unusual patterns of activity.	Manual review by AML Team of a designated patron's activity in the Report.	Recorded in central (CURA) Patron Risk Register.
Direct Transfer between customer accounts	Report from SYCO - Direct Transfer Report	Betting Account Activity	Weekly	Review of intra-patron transfers to identify unusual patterns of activity.	Manual review of a designated patron's activity in the Report to identify triggers and manual analysis against SYCO to identify anything suspicious.	Recorded in central (CURA) Risk Register. Recorded on paper report.
Screening the names of customers	Data matching between SYCO Data and	Account Activity / Crown Rewards and other Crown	Daily	Review of results of screening customer names against PEP and SDN lists.	Manual review of alerts generated by Dow Jones system.	Results stored in Dow Jones system and where appropriate,

Activity/attribute monitored	Method	CVIs	Frequency	Rationale/Criteria	Process followed	Recording of outcomes
	Screening provider.	assigned number to the Customer (e.g. VIP). The latter is not a designated service nor a CVI.				in a Crown secure drive
Telegraphic Transfers	Report from SYCO	Account Activity	Daily	Review of Telegraphic Transfers undertaken for customers to identify unusual patterns of activity.	Manual review of a designated patron's activity in the Report to identify triggers and manual analysis against SYCO to identify anything suspicious.	Recorded in central (CURA) Risk Register and paper reports.
Surveillance Identified Activity; Security Identified Activity	Notification from Surveillance & Security Team	Cash/ Casino Cheques/ Casino Chips / TITO / Casino Reward Cards/ Betting Account	Ad-Hoc	Review of all AML/CTF matters identified by GGM-AML.	Manual analysis of surveillance footage and SYCO to identify anything suspicious.	Recorded in central (CURA) Risk Register.
Names of known customers in RFI reports of	Data matching	N/A	Ad-Hoc	Review of activity of patrons that are subject to bankruptcy orders.	Manual review of patrons that are subject to an RFI to identify triggers	Recorded in central (CURA) Risk Register.

Activity/attribute monitored	Method	CVIs	Frequency	Rationale/Criteria	Process followed	Recording of outcomes
persons becoming bankrupt					and analysis against SYCO activity to identify anything suspicious.	
Customer Risk Occupation	Report from SYCO	N/A	Ad-Hoc	Review of customers that have been identified as having a higher risk occupation to identify unusual patterns of activity.	Manual review of patrons with specific occupations (bank employees, accountants, lawyers, public servants, tax agents, stockbrokers, PEPs or in other occupations involving the management of a third party's funds) and manual analysis against SYCO to identify anything suspicious.	Recorded in central (CURA) Risk Register and in occupation, audit report and reports to Senior Management.
Account Opening and Blocked Accounts	Report from SYCO	N/A	Ad-hoc	Review to identify unusual patterns of activity.	Manual review of accounts that are opened and/or blocked to identify anything suspicious.	Recorded in central (CURA) Risk Register.

Crown Perth appears to have a comprehensive transaction monitoring program that monitors the use of all CVIs and designated services in a

way appropriate to the ML/TF risks faced and to identify complex, unusually large transactions and patterns of transactions which have no apparent economic or visible lawful purpose.

Crown Perth's monitoring is also manual, largely relying on the manual review by business operations, supported by the AML Team, of system generated reports to identify triggers in customer activity. The customer that is the subject of the trigger's activity is then subsequently manually reviewed through an analysis of business systems and surveillance footage (where available and appropriate) to assess activity.

The manual review to identify triggers in Perth is also based and heavily reliant upon the reviewer's experience and knowledge, it is therefore not standardised and consistent.

The outcomes of the manual review to identify triggers and the subsequent analysis and decision making are recorded and retained within a risk register where an entry in CURA is required. For example, if a trigger is investigated and then ruled out as suspicious or concerning by the AML Team, a risk profile or risk entry may not be warranted in CURA. The relevant paper report will be ticked, signed and dated to confirm the review occurred.

This means the recording of monitoring activity and outcomes is systematic and there is a systematic way to search previous monitoring activity to identify trends or patterns not detected by triggers.

The use of manual review at the trigger identification stage of the monitoring process, whilst apparently effective, is time consuming and means skilled resources are undertaking activity that could be systemised, thereby freeing the skilled resource to focus on more value-add type activities in the trigger review.

Variations between Melbourne and Perth

Crown Perth appears to have a transaction monitoring program that is broadly consistent with the monitoring undertaken by Melbourne.

Initialism's review identified a number of variations between the two monitoring programs which are as a result of variations in gaming regulations in Victoria and Western Australia.

Perth currently has a more centralised approach to recording the outcomes of monitoring activity.

Report Data

Initialism reviewed the reports used by Crown to identify triggers to understand the level of data that was currently available and how it was and could be used to identify triggers.

Initialism's analysis of the reports used by Crown identified the availability of a number of data points/elements are available within the reports which may not be being used by current monitoring activity and would support/enhance the areas of review set out in Annexure F of the AML/CTF Program.

The data currently available could be leveraged to enhance the monitoring process:

- The data identified to support refined monitoring would support Crown reducing the false positives and allow Crown to more finely tune the monitoring based on the customer, the activity value and other data points.

Report Type	Data in Report	Refinement of Report
Cash Transactions Report	- Patron details including ID - Transaction references - Amount and In/Out - Crown Licensee details	Refine Monitoring: - Patron details - Amount and In/Out
Gaming Cheque Report	- Cheque number - Cheque Status - Patron Number & Name - Date of Issue - Licensee details - Reason (code) - Description (code) - Amount	Refine Monitoring: - Patron name and number - Amount - Reason/Description
Buy-ins Report	- Gaming Table Ref - Reward Card Usage - Date /Time - Patron Number - GUSP ID - Amount - Cash/Chip/Cheque	Refine Monitoring: - Gaming Table Ref - Patron Number - Amount - Cash/Chip/Cheque
EGM / ETG Activity Report	**EGM** - Location of EGM - Turnover - Ticket In Amount - Ticket Out Amount - Metered Notes to Stacker - Metered Coins to Cashbox	**EGM** Refine Monitoring: - Metered Notes to Stacker - Stacker + Cashbox + Ticket in Amount - Turnover **ETG**

Report Type	Data in Report	Refinement of Report
	• Stacker + Cashbox + Ticket in Amount • Ratio (Cash to Ticket In) **ETG** • Location of ETG • Turnover • Cash In Amount • Ticket In Amount • Ticket Out Amount	Refine Monitoring: • Ticket In /Ticket Out Amount • Turnover
Cancel Credits and Jackpots Report	• Game Name • EGM Ref • Time • Amount • Patron Name • Rewards Card No • Rewards Card Tier • Payment details (Cash/Cheque/Chips/DAB/Jackpot)	Refine Monitoring: • Rewards Card Tier • Payment details
TITO Tickets Report	• Source of TITO • Creation Date • Aged (No of Days) • Amount	Refine Monitoring: • Source of TITO • Aged (no of Days)
Foreign Currency Transactions Report	• Date • Location in Crown • Exchange Ref • Customer ID • Customer Name • Customer type (patron/staff) • Amount • Exchange Rate • Currency • AUD Value	Refine Monitoring: • Location in Crown • Currency
Higher Risk Customer Activity Report	• Patron Number • Patron Name • Activity type • Date /time • Crown Licensee number	Refine Monitoring: • Activity Type
Direct Transfer Report	• Date • Comments/Transfer details (to/from) • Document Ref • Location • Amount	Refine Monitoring: • Currency • Comments/Transfer details

Report Type	Data in Report	Refinement of Report
	• Currency • Status	
Telegraphic Transfers Report	• IFTI (yes/no) • TT Ref • TT Date • Ordering Patron Number • Ordering Patron Name • Beneficiary Patron Number • Beneficiary Patron Name • Amount (A$) • Amount (other currency)	Refine Monitoring: • Amount (other currency) • Beneficiary Patron Number/Name • Ordering Patron Number/Name • Multiple transactions to common beneficiary
Bankrupt Report	• Person ID • Name • Date of Birth • SYCO No • Status • Comments	Refine Monitoring: • N/A
Junket Program Report	• Junket Operator • Operator PID • Program Number • Key Player Name • Key Player PID • Program Status • Program Category • Program Code • Program Start Date • Program End Date • Estimated T/O • Estimated Actual Win/Loss	Refine Monitoring: • Junket Operator • Program Category

Planned TMP Developments

During the review Initialism were informed of significant developments to TMP which have been being developed by Crown's AML Team and are due to be rolled out.

The developments, Initialism were informed, include:

- The systemisation of trigger generation

- The systemisation and centralisation of report and data generation; and

- The centralisation and systemisation of TMP record keeping.

Initialism were provided with a **draft** set of scenarios and rules that Crown propose to deploy (in the same or a similar form) and note that they leverage all the current reports used for the manual process and provide coverage for all relevant CVIs and designated services.

Initialism reviewed the proposed scenarios/rules and the thresholds Crown proposes to apply.

Based on the material provided and discussions with the AML Team, it appears that the automation will be equivalent to the current manual trigger identification.

Area	Rule	Activity Count Threshold	$ Threshold	Period
Table Games	Carded Buy-In	>3	$5,000 to $9,999	<3 hours
	Un-carded Buy-In	>3	$5,000 to $9,999	Any
	Multiple Buy-In	>10	$5,000 to $9,999	Any
Use of TRTs	Ticket Redemption	TBA	$1,500 and $1,999	<24 hours
Use of Account	Cash Deposit	>1	$200,000	<24hours
	Cash Deposit/Withdrawal	>2	$200,000	24 hours
	CVI Deposit	>5	Aggregate of >$10,000	30 days
	Inward 3rd Party TT	>1	>$1	Any
	Outward 3rd Party TT	Any	>$1	Any
	International TT inward	Any	>$1	30 Days
Crown Cheques	Crown Cheque Issued – Week	>3	>$1	7 days
	Crown Cheque Issued – Month	>10	>$1	30 days

	Crown Cheque Issued - No Play	>1	>$5,000	24 hours
	Crown Cheque Issued Over Threshold	>1	>$100,000	24 hours
TITO Tickets	TITO Redemption	>1	>$5,000	72 hours
Other Customer Behaviours *UNDER REVIEW*	*Excessive Loss*	*N/A*	*>=$100,000*	*30 days*
	Excessive Junket Loss	*N/A*	*>=$100,000*	*End of Junket*
	High Risk Customers	*TBA*	*All rating activity*	*TBA*
	Excessive Cash Transaction and No Rated Play	*>1*	*>=$10,000*	*TBA*

It is noted that Crown propose to run the new 'automated' trigger identification and the manual trigger identification in parallel for a period of time. It is felt that this is appropriate as it will allow Crown to ensure that the automated system is delivering at least equivalent results as the manual review.

Crown also plan to establish a review and refine the process for automated monitoring, which will allow it to adjust the thresholds and introduce new scenarios/rules as appropriate and if data allows.