Crown Resorts

Transaction Monitoring Review

June 2021

INITIALISM

Background

Crown Melbourne Limited (**Crown Melbourne**) and Burswood Nominees Limited (ATF the Burswood Property Trust) (**Crown Perth**) (collectively, **Crown**) requested that Initialism conduct a review of their transaction monitoring programs, which form part of Crown's AML/CTF Program.

Crown currently has two (2) reporting entities across two sites, Crown Melbourne and Crown Perth. Whilst not specifically addressing Crown Sydney, where appropriate, this report makes reference to the transaction monitoring activity planned for Crown Sydney.

The purpose of the review is to assess the appropriateness and adequacy of Crown's approach to monitoring of customer activity undertaken to comply with its ongoing customer due diligence obligations under the Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Act and AML/CTF Rules 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 Crown's AML/CTF Program and supporting documented policies;
- Process walk-throughs and interviews with Crown personnel; and
- Review of Crown's day to day operations to assess the effectiveness of the monitoring of activity to identify unusual behaviour.

Limitations

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.

Initialism's findings, observations, and recommendations should be read in the context of the scope of work. Where possible, Crown personnel representations have been independently verified. However, some findings within this report may have been prepared on the basis of Crown representations that have not been independently tested.

Table of Contents

Executive Summary

Transaction monitoring is a key obligation placed on Reporting Entities, including Crown, by the AML/CTF Act and is fundamental to the Objects of the AML/CTF Act, which include:

> *to provide for measures to detect, deter and disrupt money laundering, the financing of terrorism, and other serious financial crimes; and*
>
> *to provide relevant Australian government bodies and their international counterparts with the information they need to investigate and prosecute money laundering offences, offences constituted by the financing of terrorism, and other serious crimes; and*
>
> *to support cooperation and collaboration among reporting entities, AUSTRAC and other government agencies, particularly law enforcement agencies, to detect, deter and disrupt money laundering, the financing of terrorism, and other serious crimes.*

The importance of the obligation for Reporting Entities to monitor customer activity to identify unusual and potentially suspicious matters is underscored by the fact that Section 36(1) of the AML/CTF Act, which sets out the requirement to monitor customer activity, is a stand-alone civil penalty provision.

Section 36(1) of the AML/CTF Act requires Crown to monitor customers when providing a designated service to identify, mitigate, and manage the risk that designated services might, inadvertently or otherwise, facilitate money laundering or the financing of terrorism.

As a result of our review, Initialism is of the opinion that Crown is monitoring its customers who it is providing designated services to for the purposes of identifying, mitigating and managing the risk of a customer's use of the designated services being involved in or facilitating money laundering or terrorist financing and is therefore meeting its obligations under section 36(1) of the AML/CTF Act.

This opinion is also supported by the understanding that the AML/CTF Act does not require Crown, along with every other Reporting Entity, to ever be in a position to entirely eliminate the risk that it may be exploited for the purposes of laundering money or financing terrorism.

The AML/CTF Act does however require Crown to identify, mitigate, and manage the risk that Crown's provision of designated services might, whether inadvertently or otherwise, involve or facilitate money laundering or terrorism financing. In so doing, Crown is supporting meeting its regulatory obligation to report suspicious matters to AUSTRAC where its risk-based monitoring identifies customer behaviour or activity deemed to be a suspicious matter reporting obligation pursuant to Section 41 of the AML/CTF Act.

Section 36 of the AML/CTF Act is supported by sub-paragraphs 15.4 to 15.7 of Chapter 15 of the AML/CTF Rules. Sub-paragraphs 15.4 to 15.7 of the AML/CTF Rules require Reporting Entities, including Crown, to have a transaction monitoring program as part of their AML/CTF program that:

- Includes appropriate risk-based systems and controls to monitor the transactions of customers;
- Has the purpose of identifying suspicious activity; and
- Has regard to complex, unusual large transactions and unusual patterns of transactions, which have no apparent economic or visible lawful purpose.

As a result of our review, Initialism is also of the opinion that Crown is meeting the requirements of Chapter 15 of the AML/CTF Rules, as the customer monitoring undertaken is documented in Part A of the AML/CTF

Program. Crown's transaction monitoring program includes appropriate systems and controls to undertake monitoring to facilitate the identification of suspicious matters and the monitoring techniques deployed seek to identify complex, unusually large transactions and patterns of transactions which have no apparent economic or visible lawful purpose.

Crown has appropriately focused transaction monitoring within its transaction monitoring programs on the financial activity and transactions related to its provision of designated services, with a particular focus on the acquisition and redemption of Casino Value Instruments (CVIs), including chips, tokens, gaming tickets, cheques, and gaming accounts. Crown's transaction monitoring program leverages a series of reports from business systems and these reports cover the activity and use of all relevant CVIs and gaming accounts.

The extent to which Crown's monitoring capability covers all aspects of its interactions with its customers is impacted by exemptions under the AML/CTF Rules which do not require the collection and verification of identification information for customers accessing a designated service under $10,000. This exemption ringfences monitoring to customers using a Crown Rewards card when gambling and therefore creates limitations on the ability to monitor uncarded play below the $10,000 threshold by customers who are not Crown Rewards members or Crown Rewards members that choose not to use their Crown Rewards card when gambling below $10,000. Patrons undertaking gaming and gambling activities in amounts less than $10,000 can remain anonymous to Crown by virtue of the exemption granted under the AML/CTF Rules.

One vulnerability previously identified through a separate review into the Riverbank and Southbank bank account activity is the use of Crown's bank accounts potentially to launder money when they are used by patrons to fund gaming activity or repay debts owed to Crown as a result of gaming activity. Initialism understands that Crown plans to monitor activity through its bank accounts via an automated monitoring process. However, it is recognised that Crown's ability to monitor patron activity through its bank accounts is limited to the information able to be provided by its bankers.

Initialism also understands that Crown have prohibited the acceptance of certain types of transactions through their bank accounts, including cash deposits and deposits from third parties, which are set out in the Return of Funds Policy . Initialism has further established that Crown currently monitors compliance with these prohibitions. Crown have also developed manual monitoring, as well as Unusual Inbound Telegraphic Transfer Rules in its automated monitoring.

Crown has also undertaken significant work to assess relevant money laundering and terrorist financing typologies from authoritative sources such as the Financial Action Task Force (FATF), AUSTRAC, Canada's FIU - FINTRAC, The UK Gambling Commission, and the American Gaming Association (AGA). This work identified over 50 separate typologies related to money laundering and terrorist financing involving a casino and has been used to assess and refine Crown's transaction monitoring program.

Crown has refined and evolved its transaction monitoring program to address the findings of Initialism's review in 2019. Since Initialism's last review in 2019, Crown has moved from largely relying on the manual review of system-generated reports to identify unusual customer activity to a blend of manual and automated monitoring.

The manual report-based monitoring activity identified in 2019 has been largely retained but is now standardised and consistent at an enterprise level, rather than at a Crown entity level.

Crown's manual monitoring is now also being supplemented by automated monitoring, which has evolved from the planned automated monitoring foreshadowed in Initialism's 2019 review report.

Initialism has also established that Crown has plans in place to further enhance its automated monitoring and in doing so further reduce its reliance on manual report monitoring.

Both Crown's manual and automated monitoring source data from the SYCO system, which acts as the single source of truth for financial transactions related to gaming activity.

SYCO (and the upstream systems) feeds are, in part, dependent on the manual input of data, gaming activity and customer information by Crown's staff. This manual (human) input of data could be a vulnerability to Crown's transaction monitoring processes if not applied in a uniform and consistent manner however Initialism acknowledges that the manual input of data and information is central to Crown's operations.

Since 2019, Crown have also introduced consistent and systematic recording of monitoring activity as well as the case management and disposition of monitoring alerts and outcomes. Whilst the recording of monitoring has improved, Initialism has been made aware of continued improvement through the deployment of Unifi.

In addition, in Q4 2020, Crown increased staff awareness of money laundering and terrorism financing "red-flags" relevant to casino activity. This has resulted in an increase in Unusual Activity Reports (UARs) from staff in Q1 2021 compared with Q1 2020, with 1,035 UARs lodged in Q1 2021, of which 776 were received from front line staff. This increased level of UAR reporting is soon to be supported by an automated form which staff complete and is systematically provided to the AML Team responsible for monitoring.

The AML Team responsible for monitoring has increased from 2 staff in 2019 to 10 staff in early 2021. Whilst it is recognised that this is a significant increase in head count, it is also anticipated that additional specialist resources will be required as the automated monitoring is further built out.

To ensure that current monitoring continues to evolve, Crown must ensure that it continues to increase the appropriately skilled resources available to manage the outputs of its monitoring activity and ensure that current monitoring and planned refinements to monitoring are not adversely impacted by resource constraints.

Initialism has also made additional observations in relation to the manual and automated monitoring processes which should be considered by Crown.

Initialism also understands that the transaction monitoring undertaken by Crown for Melbourne and Perth, excluding the monitoring of Electronic Gaming Machines (EGMs), will also be deployed for Sydney as and when required.

Overview of Recommendations and Observations

As a result of its review, Initialism make the following observations and recommendations for consideration by Crown:

Area	Recommendation/Observation
Investigation Report Guidelines	Crown should update the Guidelines to state the minimum requirements in accordance with Joint AML/CTF Policy and Procedures and should include the other elements to be undertaken as relevant to the circumstances as additional measures, if it is an expectation that the person who submitted the form is required to have completed the required ECDD.
Investigation Report Guidelines	Crown should revise the document to clearly set out which staff are required to follow the procedure.
[redacted]	[redacted]
Resourcing	Crown must ensure that it continues to increase the appropriately skilled resources available to manage the outputs of its monitoring activity and ensure that current monitoring and planned refinements to monitoring are not adversely impacted by resource constraints.

Obligation to Monitor Customers

Transaction monitoring is a key obligation placed on Reporting Entities, including Crown, by the AML/CTF Act and is fundamental to the Objects of the AML/CTF Act, which include:

> *to provide for measures to detect, deter and disrupt money laundering, the financing of terrorism, and other serious financial crimes; and*
>
> *to provide relevant Australian government bodies and their international counterparts with the information they need to investigate and prosecute money laundering offences, offences constituted by the financing of terrorism, and other serious crimes; and*
>
> *to support cooperation and collaboration among reporting entities, AUSTRAC and other government agencies, particularly law enforcement agencies, to detect, deter and disrupt money laundering, the financing of terrorism, and other serious crimes.*

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 for a reporting entity such as Crown 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 importance of the obligation for Reporting Entities to monitor customer activity to identify unusual and potentially suspicious matters is underscored by the fact that Section 36(1) of the AML/CTF Act, which sets out the requirement to monitor customer activity, is a stand-alone civil penalty provision.

The AML/CTF 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 sets out requirements related to transaction monitoring, stating:

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 AML/CTF Rules ultimately define the scope of the transaction monitoring program. The AML/CTF Rules establish that the transaction monitoring program should be documented as part of the AML/CTF Program and should 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.

Chapter 10 of the AML/CTF Rules (10.1) provides exemptions which limit the capacity of a casino to monitor transactions.

Sub-paragraph 10.1.4 permits a casino, including Crown, not to undertake customer due diligence when providing one or more of the gambling designated services when the amount is less than $10,000.

Initialism understands that not needing to identify and verify the identity of customers who gamble less than $10,000 impacts Crown's ability to monitor the activity of customers that are not Crown Rewards members or who choose not to use their Crown Rewards card when gambling under $10,000.

Initialism have used the requirements set out by the AML/CTF Act and AML/CTF Rules as part of the basis for the review and for establishing Initialism's opinion as to the adequacy of Crown's transaction monitoring program.

AML/CTF Designated Services

The AML/CTF Act and Rules require Crown's transaction monitoring program be focused on the provision of services designated. Each Crown Entity provides the following Designated Services under Table 1 and Table 3 of Section 6 and Item 3 and 4 of Section 46 of the AML/CTF Act:

Table 1

Item 31	accepting an instruction as a non-financier; and
Item 32	receiving an instruction as a non-financier.

Table 3

Item 1	receiving or accepting a bet placed or made by a person;
Item 2	placing or making a bet on behalf of a person;
Item 3	introducing a person who wishes to make or place a bet to another person who is willing to receive or accept the bet;
Item 4	*paying out winnings in respect of a bet;*
Item 6	accepting the entry of a person into a game where that game is played for money or anything else of value; the game is a game of chance or of mixed chance and skill;
Item 7	exchanging money or digital currency for gaming chips / tokens / betting instruments;
Item 8	exchanging gaming chips / tokens / betting instruments for money or digital currency;
Item 9	*paying out winnings, or awarding a prize, in respect of a game where that game is played for money or anything else of value; the game is a game of chance or of mixed chance and skill;*
Items 11-13	*in the capacity of Account Provider:* opening an Account; or allowing a person to be a signatory on an Account; or allowing a transaction to be conducted in relation to the Account, *where the Account in respect of one of the items above, and the purpose, or one of the purposes, is to facilitate the provision of one of the services as specified in Table 3 of section 6 of the Act; and*
Item 14	*foreign exchange transactions.*

Initialism has also used the AML/CTF Act designated services provided by Crown as part of the basis for the review of Crown's transaction monitoring program, including the adequacy of Crown's Part A Program and associated monitoring procedures.

Casino Value Instruments (CVIs)

Crown's provision of designated services involves the use of one or more Casino Value Instruments (CVIs). The following CVIs are used by Crown to provide designated services:

Casino Value Instrument (CVI)	Description
Cash	Physical currency (domestic and foreign currency).
Casino Chip	Casino chips are issued by casinos and used in lieu of cash in gaming transactions between the house and players. Chips are round and marked with the denomination and name of the casino and are negotiable within the casino.
Gaming Tickets (TITO)	Ticket In Ticket Out (TITO) technology works with the EGM to print a bar coded ticket for payouts when the collect button is pressed. TITOs can be inserted into a compatible EGM for credit, presented at the cashier for processing of payout, or inserted into a Credit Redemption Terminal (CRT) for the player to retrieve their funds.
Casino Cheque	Cheque drawn on the casino's own bank account.
Casino Reward Card	Card records spending activity of a patron in the casino.
Betting/Gaming Account	Account provided by the casino where patrons can hold $ value.

Initialism's review has considered the use of CVIs during the provision of designated services when reviewing Crown's transaction monitoring program. The results can be found in the Manual Monitoring and Automated Monitoring and the Review of Monitoring Alignment to Casino ML/TF Typologies sections of this report.

In addition, Initialism has reviewed the monitoring of methods used by Crown to receive and remit funds to customers, including electronic funds transfer instructions (telegraphic transfers) from Crown's bank account to and from patrons.

Telegraphic transfers to and from Crown controlled bank accounts are an important activity from a money laundering and terrorist financing risk perspective and therefore require appropriate monitoring. However, it is recognised that Crown's ability to monitor patron telegraphic transfer activity is limited to the information able to be provided by its bankers and due to the extent of information available , the monitoring by Crown will be more limited than the monitoring possible by the bank receiving and sending the telegraphic transfers.

Notwithstanding this Crown have developed manual monitoring by the VIP Team set out in the Bank Statement Monitoring Policy[1] and the Crown AML Manual Bank Statement Review Guidelines[2], as well as developing Unusual Inbound Telegraphic Transfer Rules in its automated monitoring.

[1] Bank Statement Monitoring Policy – 16th November 2020

[2] Crown AML/Manual Bank Statement Review Guidelines – Version 1.2 13th April 2021.