STATEMENT OF NEIL GEORGE JEANS – RFS – Initialism - 001

ANNEX H

Crown Resorts

Transaction Monitoring Review

April 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 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 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. Initialism has further established that Crown currently monitors compliance with these prohibitions via the Cash Transaction Report and the Telegraphic Transfer Report as part of manual transaction monitoring processes it has in place.

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 planned 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 a [X] fold increase in Unusual Activity Reports from staff in Q1 2021 compared with Q1 2020. 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 [X] 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.

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 by its nature, will be different from the monitoring possible by the bank receiving and sending the telegraphic transfers.

ML/TF Typologies

Authoritative money laundering and terrorist financing typologies and case studies provide an important additional source of information regarding the vulnerability of Crown to ML/TF risk. The following is a summary of the relevant ML/TF typologies to casinos, including Crown, 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).

51 separate typology themes for money laundering and terrorist financing involving a casino have been identified:

Typology Source	Theme	Typology Indicators
AGA AML Best Practices 2019- 2020 (p. 22)	Account Details	Multiple gaming accounts being set up from the same physical address.
FATF – Casino Typologies Report (2009) p. 39, 40/ (Points 128) AGA AML Best Practices 2019- 2020 (p. 19, 22)	Buying Winnings	> Buying winning lottery tickets / jackpots > Customers watching/hanging around jackpots sites but not participating in gambling. > Un-carded patrons with large jackpot winnings > Ticket redemption by an individual that is not known to have placed the initial bet.
FATF - Casino Typologies Report (2009) p. 31 , 35, 36 AGA AML Best Practices 2019- 2020 (p. 22-24) FINTRAC - Money Laundering and Terrorist Financing Indicators - Casinos (Jan 2019) UK Gambling Commission - The prevention of money laundering and combating the financing of terrorism (2020)	Change in Behaviour	> Noticeable spending/betting pattern changes > Dramatic or rapid increase in size and frequency of transactions for regular account holder > Abrupt change in account activity.
FINTRAC - Money Laundering and Terrorist Financing Indicators - Casinos (Jan 2019)	Change in Behaviour - Dormant Account	> An inactive account begins to see financial activity (e.g. deposits, wire transfers, withdrawals).

Typology Source	Theme	Typology Indicators
FATF – Casino Typologies Report (2009) p. 28, 32, 41 AUSTRAC Typologies and Case Studies Report 2007	Cheques - Inbound	> Frequent deposits of gaming cheques followed by immediate withdrawal of funds in cash. > Use of personal cheques, bank cheques and travellers cheques to purchase casino chips > Bank drafts/cheques cashed in for foreign currency
FATF – Casino Typologies Report (2009) p. 29 FINTRAC - Money Laundering and Terrorist Financing Indicators - Casinos (Jan 2019) AUSTRAC Typologies and Case Studies Report 2007	Cheques - outbound	> Casino cheques payable to cash - High-value casino cheques payable to cash have been observed in secondary circulation as bearer negotiable instruments > Depositing multiple large amounts of cash and receiving multiple cheques drawn on that account > Requests for casino cheques from foreign currency > Structuring Cheque Withdrawals > Any casino transaction of $3,000 or more when an individual receives payment in casino cheques made out to third parties or without a specified payee. > Cheque issued to a family member of the person
FATF – Casino Typologies Report (2009) p. 29, 35 , 40	Combine Winnings	Combining winnings and cash into casino cheques / Cashing in winnings in a multiple combination of chips, cheque and cash
AGA AML Best Practices 2019- 2020 (p. 22)	Customer Collusion	Patrons pass a large quantity of chips, cash, or TITO tickets between themselves, in an apparent effort to conceal the ownership of the chips, cash, or TITO tickets.
AGA AML Best Practices 2019- 2020 (p. 22)	Customer exiting venue with significant amount of chips	A patron leaves the casino floor with a significant amount of chips in his possession without offsetting chip redemptions or chip buy-ins at another table, and there is no known disposition or whereabouts of the chips, although this may not be deemed suspicious if there is a reasonable, experience-based expectation that the patron will return to the casino in the near future.
FATF – Casino Typologies Report (2009) p. 36, 39 UK Gambling Commission - The prevention of money laundering and combating the financing of terrorism	Deposit Account Usage	> Use of casino account as a savings account > Account activity with little or no gambling activity

Typology Source	Theme	Typology Indicators
FATF - Casino Typologies Report (2009) p. 30, 32, 34, 39, 53 AGA AML Best Practices 2019- 2020 (p. 22) FINTRAC - Money Laundering and Terrorist Financing Indicators - Casinos (Jan 2019) UK Gambling Commission - The prevention of money laundering and combating the financing of terrorism (2020)	Doubts on SoF/SoW	> Unexplained SoW/SoF and/or activity inconsistent with financial situation/customer profile > Source of funds for buy-in not disclosed > Transaction/s are inconsistent with the customer's profile - appears to be living beyond their means or financial position, large/rapid movement of funds > A patron deposits large sums of cash into a front money account but the known occupation is not a cash intensive business. > No verification of VIP's Source of funds > Open source documents show company owned by VIP could not have generated income sufficient to sustain his gambling losses
FATF - Casino Typologies Report (2009) p. 32	Employee Collusion	> Casino staff bribed to facilitate money laundering > Falsifying player ratings to legitimise criminal proceeds
FATF – Casino Typologies Report (2009) p. 42 / Case 20	Employee Collusion, Training	> Contact between patrons and casino staff outside of the casino > Customer befriending/attempting to befriend casino employees. > Casino Employees not filing suspicious reports on transactions (Corruption or Lack of Training)
FATF - Casino Typologies Report (2009) p. 31, 32, 39 (Point 129) FINTRAC - Money Laundering and Terrorist Financing Indicators - Casinos (Jan 2019) AGA AML Best Practices 2019- 2020 (p. 22) AUSTRAC Typologies and Case Studies Report 2007 UK Gambling Commission - The prevention of money laundering and combating the financing of terrorism (2020)	Even Betting	> Frequent even-money wagering when conducted by a pair of betters covering both sides of an even bet / Parallel Even money betting > Acquaintances bet against each other in even-money games, and it appears that they are intentionally losing to one of the parties. > Betting against associates / intentional losses

Typology Source	Theme	Typology Indicators
FATF – Casino Typologies Report (2009) p. 53 (Points 172) UK Gambling Commission - The prevention of money laundering and combating the financing of terrorism (2020)	Excessive Losses	VIP Player with Excessive Losses
FINTRAC - Money Laundering and Terrorist Financing Indicators - Casinos (Jan 2019)	Foreign Bank Accounts	> Use of multiple foreign bank accounts for no apparent reason.
FATF – Casino Typologies Report (2009) p. 41 / (Points 135) UK Gambling Commission - The prevention of money laundering and combating the financing of terrorism (2020)	Foreign Currency	Casino play is undertaken in foreign currency
FATF – Casino Typologies Report (2009) p. 41 / (Points 134)	Foreign Currency - Structuring	Structured currency exchanges
FATF – Casino Typologies Report (2009) p. 41, 43 / (Points 132, 133) UK Gambling Commission - The prevention of money laundering and combating the financing of terrorism (2020)	Foreign Currency - Large Transactions	> Conversion of large sums of foreign currency > Dramatic or rapid increases in size and frequency of currency exchange transactions for regular account holders. > Large, one-off, or frequent currency exchanges for customers not known to the casino
FATF – Casino Typologies Report (2009) p. 41	Foreign Currency - NCRP	Currency exchanges with little or no gambling activity
FATF - Casino Typologies Report (2009) p. 31 UK Gambling Commission - The prevention of money laundering and combating the financing of terrorism (2020)	Gaming Machine	> Customers claiming a high level of gaming machine payouts > Inserting funds into gaming machines and immediately claiming those funds as credits

Typology Source	Theme	Typology Indicators
FINTRAC - Money Laundering and Terrorist Financing Indicators - Casinos (Jan 2019) AGA AML Best Practices 2019- 2020 (p. 21) FATF – Casino Typologies Report (2009) p. 31, 36	Gaming Machine - Bill Stuffing NCRP	> Client puts money into slot machines and claims accumulated credits as a jackpot win. > Placing currency in a slot machine, then cashing out after minimal or no play and redeeming the TITO ticket at a kiosk on the gaming floor ("bill stuffing"). > Customers frequently inserting substantial amounts of banknotes in gaming machines that have high payout percentages and do not play "max bet" to limit chances of significant losses or wins, thereby accumulating gaming credits with minimal play
FATF – Casino Typologies Report (2009) p. 29, 30	Gift Cards and Certificates	> Purchase of large numbers of 'casino gift certificates'. Casino Gift Certificates can be redeemed by 3rd parties – distancing the money launderer from illicit funds > Purchase of casino reward cards – Use of illicit funds to purchase casino reward cards from legitimate customers paying them a premium above the value of a reward > Reward cards were purchased with illicit funds and were then traded for gold coins in the Casino Store
FATF – Casino Typologies Report (2009) p. 36, 43 FINTRAC - Money Laundering and Terrorist Financing Indicators - Casinos (Jan 2019) AGA AML Best Practices 2019- 2020 (p. 23)	High Risk Jurisdiction	> Transactions with jurisdictions that are known to be at a higher risk of ML/TF or countries deemed high risk or non-cooperative by the Financial Action Task Force.
FATF - Casino Typologies Report (2009) p. 32	High Volume	High volume of transactions within a short period
FATF - Casino Typologies Report (2009) p. 32 , 34, 35 , 39, 45, 52. (Points 167) FINTRAC - Money Laundering and Terrorist Financing Indicators - Casinos (Jan 2019) AGA AML Best Practices 2019- 2020 (p. 22, 23)	Identification	> Customer due diligence challenges, e.g. refusals, false documents, one-offs, tourists passing trade. Players refusing to give identification > Use of altered/fraudulent or stolen identification to conceal identity. > Client produces apparently false/counterfeit identification. > Customer name and name of account do not match > Associations with multiple accounts under multiple names or is known to use multiple names
FATF – Casino Typologies Report (2009) p. 29, 32	Inter-Casino	> Casino chips from one casino utilised in another associated casino. > Requests for credit transfers to other casinos

Typology Source	Theme	Typology Indicators
FATF – Casino Typologies Report (2009) p. 43 - 52	Junkets	> Junket tours where funds can be concealed amongst the pool for the group > Junket Key Players accepted without having to complete Source of Funds > Use of an Junket Operator to move funds and purchase chips > Use of third parties to move illicit funds > Use of representatives/ third parties to conduct cash buy-in > Use of Junket Dead Chips > Junket chips redeemed without any gambling activity > Buy -in of junket chips by a person whose occupation is not commensurate with the buy-in value > Player frequently requesting cheques from junket operator below threshold amounts > Junket issuing cheques to rival casinos
FATF – Casino Typologies Report (2009) p. 32, 36, 43, 54 AGA AML Best Practices 2019- 2020 (p. 19) FINTRAC - Money Laundering and Terrorist Financing Indicators - Casinos (Jan 2020) AUSTRAC Typologies and Case Studies Report 2007	Large Transactions	> Large amounts of cash deposited from unexplained sources > Gambling millions of dollars in cash, mostly carried in to casino in duffle bags > Patrons with Large Cash-out transactions with limited cash-in transactions, which cannot be reasonably explained through transaction review (Little or no gaming) > Client purchases large volume of chips with cash, participates in limited gambling activity with the intention of creating a perception of significant gambling, and then cashes the chips for a casino cheque. > Use of an intermediary to make large cash deposits > casino staff view very high cash use or large deposits and withdrawals by VIPs, and especially within VIP rooms, as 'normal'
AGA AML Best Practices 2019- 2020 (p. 24) UK Gambling Commission - The prevention of money laundering and combating the financing of terrorism (2020)	LEA Enquiry	Law enforcement or regulatory agencies deliver to the casino a formal request for records concerning the patron.
FATF – Casino Typologies Report (2009) p. 53 (Points 172)	Line of Credit	Casino extending to VIP line of credit (In $USD Millions)

Typology Source	Theme	Typology Indicators
FATF – Casino Typologies Report (2009) p. 39 AGA AML Best Practices 2019- 2020 (p. 24)	No Apparent Business Purpose	> Transfers with no apparent business or lawful purpose > A patron provides a wire transfer, cashier's check, or other form of payment and such instrument reflects that the transaction is being made for a purpose other than related to gaming.
FATF – Casino Typologies Report (2009) p. 39	PEP	Requests for casino accounts from Politically Exposed Persons (PEPs)
FATF - Casino Typologies Report (2009) p. 34 / (Points 116) / (Points 118) / p. 35	Refining	> Refining using the cashier's desk > launderers pay low denomination cash into their casino accounts and withdrawn funds with cash of higher denominations > Use of casino account for refining – launderers pay low denomination cash into their casino accounts and withdrawn funds with cash of higher denominations > Exchanging large quantities of quarters from non-gaming proceeds for paper currency > Client exchanges small denomination bank notes for large denomination bank notes, chip purchase vouchers or cheques.
FATF - Casino Typologies Report (2009) p. 32, 35 FINTRAC - Money Laundering and Terrorist Financing Indicators - Casinos (Jan 2019)	Refining - Possession of Small Value Denominations	> Customer in possession of large amounts of coinage or bills. > Presenting a large amount of money, but in small denominations ($1, $5, $10, and $20)
AGA AML Best Practices 2019- 2020 (p. 22) AUSTRAC Typologies and Case Studies Report 2007	Safe Deposit Box	> A patron with a safe-deposit box connected to the poker room accesses that safe-deposit box with a frequency that is disproportionately high when compared to the time and frequency of his or her poker play. > use of safety deposit box to store large amounts of cash

Typology Source	Theme	Typology Indicators
FATF – Casino Typologies Report (2009) p. 32, 34, 35, 38, 40 FINTRAC - Money Laundering and Terrorist Financing Indicators - Casinos (Jan 2019) AGA AML Best Practices 2019- 2020 (p. 22) AUSTRAC Typologies and Case Studies Report 2007 UK Gambling Commission - Prevention of ML and Combating TF	Structuring	> Frequent transactions just under thresholds – buy in, cash out, cash deposit, wire transfer and currency exchange > Customer conducts several transactions under reporting thresholds over several shift changes > Requests for winnings in separate cash or chip amounts under reporting threshold > Customer moving from table to table or room to room before the wagering amounts reach the reporting threshold > Multiple cheques being requested or drawn on account. > Patrons with large cash-out transactions (in the aggregate) with little or no CTR "out" filings. > Patrons with cash transactions, including aggregated transactions, that are just below the CTR reporting threshold.
AGA AML Best Practices 2019- 2020 (p. 24)	Suspicious Customer behaviour	> Client makes statements about involvement in criminal activities. > Client conducts transactions at different physical locations, or approaches different staff. > Client is evasive/nervous/defensive > There is evidence that the client has been dishonest/misleading when asked for information > Client is unable or unwilling to provide information about source of funds/wealth or purpose of transaction
FINTRAC - Money Laundering and Terrorist Financing Indicators - Casinos (Jan 2019)	Terrorism Financing	> Client identified by media or law enforcement as having travelled, attempted or intended to travel to high-risk jurisdictions > Law enforcement information provided which indicates individual(s) may be linked to a terrorist organization or terrorist activities. > Individual's online presence supports violent extremism or radicalization. > Transactions involve individual(s) identified by media and/or sanctions lists as being linked to a terrorist organization or terrorist activities.
FATF – Casino Typologies Report (2009) p. 43	Third Party - Remitters	Use of remittance agents to move funds across borders
FATF – Casino Typologies Report (2009) p. 32, 35, 43 AUSTRAC Typologies and Case Studies Report 2007	Third Party conducting Gaming Transactions	> Third party presents for all transactions but does not participate in the actual transaction > Use of third party to conduct wagering > Cash handed to third party after cash out > Use of third parties to purchase casino chips

Typology Source	Theme	Typology Indicators
FATF – Casino Typologies Report (2009) p. 39, 43 AGA AML Best Practices 2019- 2020 (p. 23)	Third Party Transactions - Gatekeepers	> Use of gatekeepers, e.g. accountants and lawyers to undertake transactions > A negotiable instrument or wire transfer is presented for the benefit of an individual and originates from a law firm account, or is from a charitable/non-profit organization or foundation, another type of trust or labor union account.
FATF – Casino Typologies Report (2009) p. 34, 43, 35, 38,39 FINTRAC - Money Laundering and Terrorist Financing Indicators - Casinos (Jan 2019) AGA AML Best Practices 2019- 2020 (p. 23) AUSTRAC Typologies and Case Studies Report 2007	Third Party Transfers	> Multiple individuals sending funds to the one beneficiary > Use of third parties to undertake structuring of deposits and wire transfers > Funds transferred from casino account to a charity fund > Transfer of company accounts to casino accounts. > Transferring funds into third party accounts. > On the VIP's behalf, Casino conducting wire transfers and direct bank to bank transfers from Corporate Accounts > Multiple deposits which are made to an account by non-account holders. > A client conducts transaction while accompanied, overseen or directed by another party. > A client makes numerous payments to unrelated parties shortly after they receive funds. > Wire transfers, deposits or payments to or from unrelated parties (foreign or domestic). > Client appears or states to be acting on behalf of another party. > Account is linked to seemingly unconnected parties. > Checks or wire transfers received for the benefit of the patron (or multiple patrons) from third parties whose connection to the patron is suspect or unclear.
FINTRAC - Money Laundering and Terrorist Financing Indicators - Casinos (Jan 2019) AGA AML Best Practices 2019- 2020 (p. 22)	Threshold Discovery	> Client enquires about opening an account with the casino and the ability to transfer the funds to other locations when you do not know the client as a regular, frequent or large volume player. > Client makes inquiries that would indicate a desire to avoid reporting. > Inquiring with race and sportsbook staff about reporting and identification thresholds either before or after a wager and possibly adjusting wagering activity to fall below the applicable thresholds. > A patron requests information about how to avoid BSA/AML reporting requirements.
FATF - Casino Typologies Report (2009) p. 32	Ticket Aging	CPV, TITO, ticket or voucher dated prior to date of redemption

Typology Source	Theme	Typology Indicators
FATF – Casino Typologies Report (2009) p. 29 – p. 30, 31, 35, 40, 45/ Case 1 / Case 3 / Case 7 AGA AML Best Practices 2019-2020 (p.19) FINTRAC - Money Laundering and Terrorist Financing Indicators - Casinos (Jan 2019) AUSTRAC Typologies and Case Studies Report 2007 UK Gambling Commission - The prevention of money laundering and combating the financing of terrorism (2020)	Transactions with NCRP	> Purchasing and cashing out chips with no gaming activity > Large Cash-in with no cash-out transactions (Little or no gaming Activity) > Client purchases large volume of chips with cash, participates in limited gambling activity with the intention of creating a perception of significant gambling, and then cashes the chips for a casino cheque. > Frequent cash out transactions with no recent gaming activity or corresponding buy-in transactions > Funds withdrawn from account shortly after being deposited > Purchasing chips or undertaking cash transaction and immediately leaves casino.
FINTRAC - Money Laundering and Terrorist Financing Indicators - Casinos (Jan 2019)	Unusual Transaction Activity	Client uses various wire deposit methods and disbursement amounts in an attempt to test the vulnerability of the system and/or account.
FINTRAC - Money Laundering and Terrorist Financing Indicators - Casinos (Jan 2019) AGA AML Best Practices 2019- 2020 (p. 23)	Unusual Transaction Activity	> A series of complicated transfers of funds that seems to be an attempt to hide the source and intended use of the funds. > Transactions displaying financial connections between individuals who have previously raised suspicion. > Transaction is unnecessarily complex for its stated purpose. > Client presents notes or financial instruments that are packed, transported or wrapped in an uncommon way. > Transaction consistent with publicly known trend in criminal activity. > Client presents musty, odd smelling or extremely dirty bills. > Client frequently exchanges small bills for larger bills. > Suspicious pattern emerges from a client's transactions (e.g. transactions take place at the same time of day).
AGA AML Best Practices 2019- 2020 (p. 23) AUSTRAC Typologies and Case Studies Report 2007	Unusual Transaction Activity - Rapid Movement of Funds	> A patron deposits funds into a front money account or receives a wire transfer, does not play a substantial amount of the funds, then requests a withdrawal or wire out. > Atypical transfers by client on an in-and-out basis, or

Typology Source	Theme	Typology Indicators
		other methods of moving funds quickly, such as a cash deposit followed immediately by a wire transfer of the funds out. > Funds transferred in and out of an account on the same day or within a relatively short period of time. > Buying chips for cash or on account, then redeeming value by way of a casino cheque, bank draft of money transfer
FATF – Casino Typologies Report (2009) p. 43, 44/ (Points 138)	Use of Credit Cards	> Laundering proceeds from stolen credit cards > Use of credit cards to conduct money laundering transactions > Use of credit cards to purchase casino chips
FATF – Casino Typologies Report (2009) p. 39, 43 AUSTRAC Typologies and Case Studies Report 2007	U-Turn Transactions	U-turn transactions occurring with funds being transferred out of country and then portions of those funds being returned

Crown's work to assess relevant money laundering and terrorist financing typologies from authoritative sources identified over 50 separate typology themes for money laundering and terrorist financing involving a casino.

Initialism separately validated the typologies work undertaken by Crown and used the typology indicators identified by Crown as part of the basis for its review of Crown's transaction monitoring program, the results of which can be found in the Review of Monitoring Alignment to Casino ML/TF Typologies section of this report.