

NOTICE OF FILING

This document was lodged electronically in the FEDERAL COURT OF AUSTRALIA (FCA) on 1/03/2022 11:01:29 AM AEDT and has been accepted for filing under the Court's Rules. Details of filing follow and important additional information about these are set out below.

Details of Filing

Document Lodged: Concise Statement
File Number: NSD134/2022
File Title: CHIEF EXECUTIVE OFFICER OF THE AUSTRALIAN TRANSACTION REPORTS AND ANALYSIS CENTRE v CROWN MELBOURNE LIMITED ACN 006 973 262 & ANOR
Registry: NEW SOUTH WALES REGISTRY - FEDERAL COURT OF AUSTRALIA



Sia Lagos

Dated: 1/03/2022 11:19:24 AM AEDT

Registrar

Important Information

As required by the Court's Rules, this Notice has been inserted as the first page of the document which has been accepted for electronic filing. It is now taken to be part of that document for the purposes of the proceeding in the Court and contains important information for all parties to that proceeding. It must be included in the document served on each of those parties.

The date and time of lodgment also shown above are the date and time that the document was received by the Court. Under the Court's Rules the date of filing of the document is the day it was lodged (if that is a business day for the Registry which accepts it and the document was received by 4.30 pm local time at that Registry) or otherwise the next working day for that Registry.



Form NCF1

CONCISE STATEMENT

**FEDERAL COURT OF AUSTRALIA
DISTRICT REGISTRY: NEW SOUTH WALES
DIVISION: COMMERCIAL AND CORPORATIONS**

NO NSD OF 2022

**CHIEF EXECUTIVE OFFICER OF THE AUSTRALIAN
TRANSACTION REPORTS AND ANALYSIS CENTRE**
Applicant

CROWN MELBOURNE LIMITED
ACN 006 973 262
First Respondent

**BURSWOOD NOMINEES LTD ATF THE BURSWOOD
PROPERTY TRUST TRADING AS CROWN PERTH**
ACN 078 250 307
Second Respondent

A. IMPORTANT FACTS GIVING RISE TO THE CLAIM

The money laundering risks of casinos

1. Crown Melbourne Ltd (**Crown Melbourne**) and Burswood Nominees Ltd (**Crown Perth**) provide designated services that are regulated by the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (the **Act**). These designated services involve higher money laundering and terrorism financing (**ML/TF**) risks:
 - a. Crown Melbourne and Crown Perth provide more than just gaming services to customers. They provide financial services that facilitate the movement of money into and out of the casino environment, including across international borders. These financial services are high value and high volume.
 - b. Cash is used extensively for gaming services at the casinos. Cash can also be transferred into and out of the casinos. The ownership of cash is less transparent than the ownership of other forms of money, and is therefore particularly vulnerable to ML/TF.
 - c. Crown Melbourne and Crown Perth move money quickly by facilitating high volume, high frequency and high value transactions 24 hours a day, 7 days a week, including across international borders.
 - d. The designated services provided to casino customers involve long and complex transactional value chains ranging from receipt of funds, account management, gaming

Filed on behalf of the Applicant, the Chief Executive Officer of
the Australian Transaction Reports and Analysis Centre

File ref: 22001484

Prepared by: Sonja Marsic
AGS lawyer within the meaning of s 551 of the *Judiciary Act*
1903

Telephone: 02 9581 7505
Lawyer's Email:
sonja.marsic@ags.gov.au

Address for Service:
Australian Government Solicitor,
Level 10, 60 Martin Pl, Sydney 2000
sonja.marsic@ags.gov.au

activities and outward disbursement of funds. These transactional chains also involve different channels and jurisdictions.

- e. Within these complex transaction chains, money used for gaming activities can be moved through further layers involving:
 - i. different and highly transferrable casino value instruments such as chips and tickets;
 - ii. multiple games, including electronic games that are not face-to-face; and
 - iii. gaming accounts.
 - f. Adding to the risk of layering through complex transaction chains, Crown Melbourne and Crown Perth facilitated the transfer of money:
 - i. between gaming accounts held in different customer names; and
 - ii. to and from third parties via gaming accounts by way of remittance through Crown bank accounts.
 - g. Crown Melbourne and Crown Perth provide designated services to higher risk customers, including to international customers through high risk junket channels and other VIP programs.
 - h. International VIP customers often relied on credit or loans provided by Crown Melbourne and Crown Perth, as a means of accessing funds on arrival at the casinos. Loans enabled funds held in foreign jurisdictions (by customers or third parties) to be used in Australia without the need for a cross-border transfer. Loans could be repaid by third parties.
 - i. Casinos are exposed to significant money laundering vulnerabilities and ML/TF typologies, including structuring, smurfing, cuckoo smurfing, offsetting, even-betting, and quick/high turnover with minimal betting. Gaming accounts can also be used to store illicit money outside the banking system.
2. In the absence of appropriate risk-based controls, these combined risks made Crown Melbourne and Crown Perth vulnerable to criminal exploitation. This is because money could be moved into and out of the casinos, and within the casinos, in ways that lacked transparency as to the source and ownership of funds.

AML/CTF Programs

3. To manage these ML/TF risks, Crown Melbourne and Crown Perth were required by s 81 of the Act to adopt and maintain an Anti-Money Laundering and Counter-Terrorism Financing Program (**Program**). To meet the obligations under the Act, a reporting entity can adopt and maintain a **Standard Program**: s84 of the Act. Alternatively, reporting entities that are part of a designated business group can adopt and maintain a **Joint Program**: s85 of the Act. Standard and Joint Programs comprise a Part A and a Part B: ss84(1) and 85(1) of the Act.

Part A Programs

4. Part A of a Program must have the primary purpose of identifying, mitigating and managing the ML/TF risks reasonably faced by reporting entities with respect to designated services. Part A Programs must also meet the requirements set out in the *Anti-Money Laundering and Counter-Terrorism Financing Rules 2007* (Cth) (the **Rules**): ss84(2) and 85(2) of the Act (see paragraph 13 below).
5. Part A Programs are the framework through which Boards and senior management assess their ML/TF risks and determine their ML/TF risk appetite. They are the framework through which Boards

and senior management determine the risk-based controls they will apply to mitigate and manage the ML/TF risks they choose to accept.

Part B Programs

6. Part B of a Program must set out the applicable customer identification procedures (**ACIPs**) for the purposes of the application of Part 2 of the Act to customers. Part B must also meet the requirements of the Rules: ss84(3) and 85(3) (see paragraph 42 below).
7. Part B Programs set out the procedures through which a reporting entity collects and verifies information to enable it to know its customers (**KYC information**). ACIPs enable a reporting entity to verify the identity of its customers and to understand and assess the ML/TF risks they pose with respect to the provision of designated services.

The contraventions of s 81 - the failures to adopt and maintain a Program

8. From 1 March 2016 to 1 November 2020, Crown Melbourne and Crown Perth each purported to adopt and maintain their own **Standard Part A and Part B Programs**. At no time did Crown Melbourne's or Crown Perth's Standard Part A and Part B Programs meet the requirements of the Act and Rules, contrary to s84 of the Act.
9. On and from 2 November 2020, Crown Melbourne and Crown Perth each purported to adopt and maintain a **Joint Part A and Part B Program**. At no time has Crown Melbourne's and Crown Perth's Joint Part A and Part B Program met the requirements of the Act and Rules, contrary to s85 of the Act.
10. A reporting entity contravenes s81 of the Act on each occasion that it provides a designated service where it does not have a Part A and Part B Program in place that meets the requirements of ss84 or 85 of the Act.
11. Crown Melbourne and Crown Perth have accordingly provided designated services in contravention of s81 on and from 1 March 2016. These contraventions are too numerous to quantify and are ongoing.
12. Crown Melbourne's and Crown Perth's non-compliance with ss81, 84 and 85 of the Act was long-standing, systemic and reflective of wholly inadequate oversight by their Boards and senior management. This non-compliance exposed Crown Melbourne and Crown Perth to the risk of being exploited by organised crime.

The Part A Program failures

13. In order to have the primary purpose of identifying, mitigating and managing the ML/TF risks reasonably faced by providing designated services (ss84(2)(a) and 85(2)(a)) and to meet the requirements of the Rules (ss84(2)(c) and 85(2)(c)), Crown Melbourne's and Crown Perth's Part A Program was required to:
 - a. include a risk methodology that was capable of appropriately identifying and assessing the ML/TF risks of the designated services they provided (paragraph 15 below);
 - b. be aligned to the ML/TF risks they reasonably faced with respect to the provision of designated services, as assessed through the risk methodology (paragraphs 16 to 18 below);
 - c. include or establish an appropriate approval and oversight framework (paragraphs 19 to 24 below);

- d. include appropriate risk-based systems and controls, capable of mitigating and managing the ML/TF risks with respect to all designated services, consistent with risk appetite (paragraphs 25 to 29 and 35 to 37 below);
- e. include a risk-based transaction monitoring program to monitor the transactions of customers and to identify suspicious matters for the purposes of s 41 of the Act (paragraph 30 below);
- f. include a risk-based enhanced customer due diligence (**ECDD**) program that applies to customers that pose higher ML/TF risks (paragraphs 31 to 32 below); and
- g. include appropriate systems and controls designed to ensure that reports required under Part 3 of the Act are given to AUSTRAC, namely suspicious matter reports (**SMRs**), threshold transaction reports (**TTRs**), and international funds transfer instructions (**IFTIs**) (paragraphs 33 to 34 below).

The Standard Part A Programs

14. From 1 March 2016 to 1 November 2020, Crown Melbourne and Crown Perth each failed to adopt and maintain a Standard Part A Program that met each of the requirements in paragraph 13 for the following reasons.

ML/TF risk assessment methodology

15. The Standard Part A Programs did not include a methodology:
- a. to appropriately assess the inherent ML/TF risks of the designated services provided: rules 8.1.3 and 8.1.4 of the Rules;
 - b. to measure the likelihood and impact of ML/TF risks with respect to designated services;
 - c. that covered all relevant risks and associated risk attributes reasonably faced by Crown Melbourne and Crown Perth with respect to designated services;
 - d. that had regard to the nature, size and complexity of the Crown Melbourne and Crown Perth businesses, including with respect to the ML/TF risks of complex designated service chains;
 - e. that had appropriate regard to the risk factors of customer, channel and jurisdiction in assessing the ML/TF risks posed by each designated service: rules 8.1.4(1), (2), (3) and (4) of the Rules; and
 - f. to assess the residual ML/TF risks of designated services, once risk-based controls had been applied: rules 8.1.3 and 8.1.4 of the Rules.

Alignment to current ML/TF risks

16. Once a reporting entity identifies the ML/TF risks it reasonably faces, and carries out an assessment of those risks in accordance with an appropriate ML/TF risk methodology, the reporting entity must align its Part A program to those risks as assessed. In aligning a Part A program to the ML/TF risks reasonably faced, a reporting entity must have regard to the nature, size and complexity of its business, and the ML/TF risks related to their designated services, customers, channels and the foreign jurisdictions with which they deal.
17. At no time were the Standard Part A Programs aligned to an appropriate assessment of the ML/TF risks reasonably faced by Crown Melbourne and Crown Perth with respect to the provision of designated services. The Risk Registers annexed to the Standard Part A Programs were fundamentally deficient, did not cover all designated services, did not include key ML/TF risks reasonably faced, and were not subject to appropriate review: rules 8.1.5(3) and (4) of the Rules.

18. Casinos operate in dynamic ML/TF risk environments. At no time did the Standard Part A Programs include appropriate risk-based systems and controls to identify significant changes in ML/TF risks and to recognise such changes for the purposes of the Part A and Part B Programs. At no time did the Standard Part A Programs include appropriate risk-based systems and controls to identify, mitigate and manage ML/TF risks arising from new designated services, channels or technologies, prior to their introduction: rule 8.1.5(5) of the Rules.

Approval and oversight

19. A reporting entity the nature, size and complexity of Crown Melbourne and Crown Perth, having regard to the ML/TF risks it reasonably faces, cannot adopt and maintain a Part A Program that has the primary purpose of identifying, mitigating and managing ML/TF risks reasonably faced with respect to the provision of designated services in the absence of a framework in the Part A program that is designed to:
- a. determine and set the reporting entity's ML/TF risk appetite;
 - b. set controls to ensure designated services are provided to customers consistently with that ML/TF risk appetite;
 - c. appropriately monitor management's performance against an appropriate ML/TF risk management framework, including the reporting entity's risk appetite;
 - d. ensure the Board receives and reviews management reports about new and emerging sources of ML/TF risk and about the measures management are taking to deal with those risks; and
 - e. establish appropriate ML/TF risk management capability frameworks, including with respect to roles and accountabilities, operational procedures, reporting lines, escalation procedures, assurance and review, and information management:

See ss81, 84(2)(a) and 84(2)(c) of the Act, rules 8.1.3, 8.1.5(4), and Part 8.4 of the Rules.

20. At no time did the Standard Part A Programs meet these requirements. As a result, the Crown Melbourne and Crown Perth Boards and senior management had no basis to be satisfied that the Standard Part A Programs were operating as intended and that they had the primary purpose of identifying, mitigating and managing the ML/TF risks reasonably faced by the provision of designated services.
21. In the face of known and serious ML/TF risks, the Board and senior management of Crown Melbourne and Crown Perth failed to set any ML/TF risk appetite through the Standard Part A Programs. They failed to adopt and maintain controls to ensure that designated services were provided within an appropriate risk appetite. They failed to adopt controls to mitigate and manage the full range of ML/TF risks across all designated services - both gaming and financial.
22. The Crown Melbourne and Crown Perth Boards and senior management failed to establish appropriate AML/CTF capabilities and failed to invest in appropriate IT systems and automated solutions. As a result, the Standard Part A Programs were not capable, by design, of operating as intended.
23. In the absence of an appropriate framework for ML/TF risk oversight, Crown Melbourne and Crown Perth provided designated services through high risk channels that were not subject to appropriate risk-based controls - including through junket channels, Crown Patron account channels, overseas deposit services and the Hotel Card Transactions channel. In the absence of appropriate controls, Crown Melbourne and Crown Perth provided designated services to high risk customers in circumstances where concerns should have been raised as to the legitimacy of

their source of wealth or source of funds. Appropriate risk-based processes were not in place to determine the ML/TF risk appetite with respect to such customers.

24. These failures in oversight resulted in serious and systemic non-compliance with the Act over many years. These failures allowed high risk customers to move money in non-transparent ways with minimal due diligence on ML/TF risks. These failures exposed Crown Melbourne and Crown Perth to the risk of being exploited by organised crime.

Risk-based systems and controls applying to all designated services to manage risk within appetite

25. Once a reporting entity identifies and assesses its inherent ML/TF risks and the Board determines ML/TF risk appetite, the reporting entity must ensure that its Part A program includes appropriate risk-based systems and controls to mitigate and manage residual risks within appetite.
26. These systems and controls must be aligned with, and proportionate to, the ML/TF risks reasonably faced by the reporting entity with respect to designated services.
27. In the absence of appropriate ML/TF risk assessments, Crown Melbourne's and Crown Perth's Standard Part A Programs were incapable by design of including appropriate risk-based systems and controls to mitigate and manage the ML/TF risks.
28. Amongst other failures, the Standard Part A Programs did not include appropriate risk-based systems and controls to appropriately identify, mitigate and manage the ML/TF risks with respect to:
- a. gaming accounts;
 - b. loans and loan repayments - including to higher risk junket operators and international VIP customers;
 - c. designated remittance services - including cross-border remittance and remittance through higher risk channels such as Crown Patron accounts, including the Southbank and Riverbank accounts;
 - d. the exchange of money for casino value instruments such as chips and tickets (and vice-versa);
 - e. table games and electronic gaming machines;
 - f. foreign currency exchange;
 - g. designated services provided in foreign currencies;
 - h. designated services involving cash;
 - i. designated services involving third parties; and
 - j. designated services provided through junket channels.
29. The Standard Part A Programs had few preventative controls designed to enable Crown Melbourne and Crown Perth to mitigate and manage its ML/TF risks in respect of these designated services. The Part A controls were predominantly detective and limited to staff observation and surveillance for unusual activity that may require SMR reporting to AUSTRAC. The Part A controls were predominantly focussed on gaming services. Higher risk financial services, that permitted money to be moved into and out of the casinos, including across international borders, were not subject to appropriate risk-based controls.

Transaction monitoring programs

30. Crown Melbourne and Crown Perth each failed to include an appropriate risk-based transaction monitoring program in their Standard Part A Programs to monitor the transactions of their customers and to identify suspicious matters, as required by Chapter 15 and rule 8.1.3 of the Rules and s 85(2)(c) of the Act as follows:
- a. As Crown Melbourne and Crown Perth failed to appropriately identify and assess the ML/TF risks of their designated services, transaction monitoring was not aligned with and proportionate to the ML/TF risks of their businesses.
 - b. The transaction monitoring programs were not capable by design of detecting well known ML/TF typologies and vulnerabilities.
 - c. The transaction monitoring programs were manual and relied heavily on staff observation and surveillance, with inadequate guidance or criteria. This also meant Crown Melbourne and Crown Perth were unable to monitor the movement of money through complex and layered transaction chains.
 - d. Manual transaction monitoring was not aligned to the nature, size and complexity of Crown Melbourne's and Crown Perth's businesses, having regard to the ML/TF risks they reasonably faced.
 - e. The transaction monitoring programs were not capable of operating as intended, due to significant deficiencies in information management systems and in the resourcing of the AML/CTF compliance function.
 - f. The transaction monitoring programs did not include appropriate risk-based systems and controls that were capable of monitoring all of the designated services provided by Crown Melbourne and Crown Perth under tables 1 and 3, s6, as listed in paragraph 28.
 - g. The transaction monitoring programs did not include appropriate risk-based systems and controls to monitor the transactions of customers who received designated services through junket channels.
 - h. The transaction monitoring programs did not include appropriate assurance processes.

Enhanced customer due diligence programs

31. Crown Melbourne's and Crown Perth's Standard Part A Programs did not include appropriate systems, controls and procedures to apply appropriate risk-based ECDD to customers who were:
- a. determined to be high ML/TF risk;
 - b. foreign politically exposed persons (**PEPs**); or
 - c. the subject of a suspicion that had arisen for the purposes of s41 of the Act
(the **ECDD triggers**).
32. This was because:
- a. The ECDD programs did not include systems, controls and procedures to identify and escalate customers rated high risk, including customers known or suspected to have connections to money laundering, and foreign PEPs.
 - b. The ECDD Programs were not capable of identifying and escalating customers who should have been rated high risk.

- i. All customers were rated low risk by default. The Part A processes for identifying and escalating customers who should not have been rated low risk were inadequate.
 - ii. The deficiencies in the Part B Programs limited Crown Melbourne's and Crown Perth's ability to identify and escalate customers who should have been reviewed to determine whether or not they were high risk.
- c. The Standard Part A Programs were not capable of consistently identifying customers who were foreign PEPs.
- d. The ECDD Programs relied upon the transaction monitoring programs to identify customers engaging in unusual or suspicious transactions, but the transaction monitoring programs were inadequate.
- e. The Standard Part A Programs did not contain procedures to escalate a customer for ECDD when a s41 suspicion had in fact arisen.
- f. The ECDD Programs did not include adequate operational procedures or guidance on the appropriate suite of risk-based ECDD measures to apply in response to specific ECDD triggers. Nor was there guidance on the criteria against which customers would be reviewed.
- g. The ECDD Programs did not include appropriate systems and controls to obtain, analyse and record source of wealth and source of funds information with respect to customers.
- h. The ECDD Programs were not supported by appropriate information management and record keeping. As well as being dispersed across multiple IT systems, customer records were also dispersed across multiple customer IDs and names, including pseudonyms. Crown Melbourne's and Crown Perth's IT and record keeping systems were not capable of providing a complete view of customers' transactions and ML/TF risk profiles for ECDD purposes.
- i. The ECDD Programs did not include appropriate systems and controls to seek senior management approval for continuing business relationships with customers, having regard to the ML/TF risks reasonably faced.
 - i. The ECDD Programs did not appropriately set out the risk appetite that was acceptable with respect to customers.
 - ii. The processes in the ECDD Program to escalate high risk customers and foreign PEPs to senior management were inadequate.
- j. There were no appropriate processes in the ECDD Programs for senior management to determine whether a transaction or transactions should be processed having regard to ML/TF risks.

Failure to have appropriate systems and controls to ensure SMR, TTR and IFTI reporting

- 33. Crown Melbourne's and Crown Perth's Standard Part A Programs did not include appropriate systems and controls designed to ensure compliance with their obligation to report SMRs, TTRs and IFTIs to AUSTRAC under ss41, 43 and 45 of Part 3 of the Act, as required by rule 8.9.1(2) of the Rules and s84(2)(c) of the Act.
- 34. The systems and controls in Part A of the Programs for Part 3 reporting were deficient because:
 - a. The policies and guidance on identifying and assessing unusual or potentially suspicious matters were inadequate. There was little to no guidance on unusual or potentially suspicious activity relating to table 1, s6 financial services.

- b. Resourcing for SMR reporting was inadequate.
- c. Dispersed data sources for customer information limited Crown's ability to understand a customer's transactional activity and to determine whether any particular activity was unusual or suspicious.
- d. There was a lack of appropriate documentation, monitoring and assurance across SMR and TTR reporting.
- e. Crown Melbourne did not make and keep complete records of all designated services involving cash, and therefore did not have appropriate systems in place to identify and report all TTRs.
- f. The processes for TTR reporting were manual.
- g. The policies and guidance relating to TTR reporting were inadequate.
- h. IFTI reporting at Crown Melbourne was not subject to appropriate assurance.
- i. SMRs, TTRs and IFTI reports relating to activity on junket programs were likely to be reported under the junket operator's name (with the junket representative as agent) rather than under the name of the junket player who conducted the transaction.

The junket channel

- 35. At all times prior to the COVID-19 border closures in March 2020, Crown Melbourne and Crown Perth provided high value designated services (both gaming and financial) through junket channels. Designated services provided through the junket channel involved complex value chains including credit, remittance, gaming accounts and gaming. Junkets involved the movement of large amounts of money across borders and through multiple bank accounts, including by third parties, remitters and overseas deposit services. The identities of persons conducting transactions through junket programs, and the source and ownership of their funds, was often obscured. A number of junket operators and representatives were reportedly connected to organised crime.
- 36. The systemic deficiencies in the Standard Part A Programs were reflected in the poor ML/TF risk management of junkets.
- 37. Crown Melbourne and Crown Perth did not carry out an appropriate ML/TF risk assessment of the higher ML/TF risks of providing designated services through the junket channel. Board and senior management oversight with respect to junkets was seriously deficient. No ML/TF risk appetite was set with respect to designated services facilitated through junkets. At no time did the Standard Part A Programs include appropriate risk-based controls to identify, mitigate and manage the ML/TF risks of designated services provided through junket channels. Instead of applying heightened risk-based controls, Crown Melbourne and Crown Perth permitted some junket operators to: operate cash administration desks in private gaming rooms; facilitate the distribution of winnings to junket players and third parties; and facilitate transactions through non-transparent Crown bank accounts.

The Joint Part A Program from 2 November 2020

- 38. Crown Melbourne and Crown Perth have commenced the process of uplifting AML/CTF controls.
- 39. In December 2021, Crown Melbourne and Crown Perth completed an enterprise wide risk assessment (**EWRA**), which rated overall inherent risk as high. The Joint Part A Program controls were not assessed as part of the EWRA because these controls are not yet comprehensively

designed and operating effectively. (However, based on the EWRA, some updates to the Joint Part A Program were approved in December 2021).

40. The Crown Melbourne and Crown Perth Boards are accordingly not yet in a position to determine their ML/TF risk appetite; and are yet to be in a position to determine the risk-based controls that must be adopted and maintained to ensure:
 - a. the ML/TF risks of all designated services are appropriately identified, mitigated and managed;
 - b. designated services are provided to customers consistent with the ML/TF risk appetite determined by the Boards; and
 - c. the full suite of both detective and preventative controls in Part A are aligned to and proportionate to the ML/TF risks reasonably faced with respect to the provision of designated services.
41. The Joint Part A Program accordingly does not yet have the primary purpose of identifying, mitigating and managing the ML/TF risks reasonably faced by providing designated services and does not comply with the requirements of the Rules: ss85(2)(a) and (c) of the Act.

The Part B Program failures

42. Part 2 of the Act, as relevantly modified by Chapter 10 and rule 14.4 of the Rules (made under s39 of the Act), required Crown Melbourne and Crown Perth to identify their customers in accordance with the ACIPs they established in Part B of their Programs. Chapter 4 of the Rules, made under s85(3)(b) of the Act, set out the relevant requirements for Part B Programs.

The Standard Part B Programs

43. From 1 March 2016 to 1 November 2020, the Standard Part B Programs did not include appropriate risk-based systems and controls that were designed to enable Crown Melbourne and Crown Perth to be reasonably satisfied, where the customer was an individual, that the customer was the individual he or she claimed to be: rule 4.2.2 of the Rules.
44. Crown Melbourne and Crown Perth applied the same 'safe harbour' ACIP to all customers, regardless of ML/TF risk.
45. Contrary to the requirements of Chapter 4 of the Rules, at no time did the Standard Part B Programs:
 - a. include risk-based systems and controls to identify customers who were not low risk at the time the ACIP was being carried out: rules 4.2.2 and 4.1.3 of the Rules;
 - b. appropriately consider the ML/TF risk posed by customer types, including customers receiving designated services through junkets, international VIP customers and foreign PEPs: rules 4.2.2, 4.1.3(1), 4.1.3(2) and 4.13.3 of the Rules;
 - c. consider the ML/TF risk posed by a customer's sources of wealth and funds: rules 4.2.2 and 4.1.3(2) of the Rules;
 - d. consider the ML/TF risk posed by the nature and purpose of the business relationship with its customers, including as appropriate, the collection of information relevant to that consideration - particularly with respect to junket operators, representatives and players: rules 4.2.2 and 4.1.3(3) of the Rules;

- e. consider the ML/TF risk posed by the types of designated services Crown Melbourne and Crown Perth provided, together with the methods or channels by which designated services were delivered: rules 4.2.2 and 4.1.3(5) and (7) of the Rules;
 - f. consider the ML/TF risk posed by the ML/TF risk factor of jurisdiction: rules 4.2.2 and 4.1.3 (7) of the Rules;
 - g. include appropriate risk-based systems and controls for Crown Melbourne and Crown Perth to determine whether additional KYC information would be collected about a customer and/or verified: rules 4.2.2, 4.2.5 and 4.2.8 of the Rules;
 - h. include ACIPs to be applied to all customers who Crown Melbourne and Crown Perth were required to identify for the purposes of Part 2 of the Act - including customers who were not subject to exemptions or customers seeking table 1, s6 financial services: section 84(3)(a); see also ss 32 and 39 of the Act; and Chapter 10 and rule 14.4 of the Rules;
 - i. include an appropriate procedure to collect information and documents about an agent of a customer (who was an individual) and did not include appropriate risk-based systems and controls to determine whether to verify (and to what extent) the identity of the agent: Part 4.11 of the Rules;
 - j. include appropriate risk-management systems to consistently determine whether a customer was a PEP, either before the provision of a designated service to the customer or as soon as practicable after the designated service has been provided: rule 4.13.1 of the Rules; and
 - k. comply with the requirements of rule 4.13.3 of the Rules with respect to PEPs.
46. The significant deficiencies in Crown Melbourne's and Crown Perth's information management systems limited their ability to know who their customers were, as at the time the ACIP was carried out: rules 4.2.2 and 15.3 of the Rules.

The Joint Part B Programs

47. On and from 2 November 2020, the Joint Part B Program has not complied with the same requirements of Chapter 4 of the Rules set out at paragraphs 43 to 46 above, in contravention of s84(3) of the Act. Risk-based systems and controls, including those set out in Part B, are yet to be assessed and uplifted.

Ongoing customer due diligence failures - 547 contraventions of s36 of the Act

48. Together, Crown Melbourne and Crown Perth failed to carry out appropriate due diligence on their customers, with a view to identifying, mitigating and managing known ML/TF risks on 547 occasions, contrary to s36 of the Act.

The 60 customers posing high ML/TF risks - 83 contraventions

49. On and from 1 March 2016, Crown Melbourne and Crown Perth provided designated services to 60 customers, in respect of whom high ML/TF risks were indicated. With respect to the 60 customers:
- a. many were junket operators, junket representatives or junket players;
 - b. many were foreign PEPs, or a person that Crown Melbourne or Crown Perth otherwise determined to be high risk;
 - c. many were connected to other Crown Melbourne or Crown Perth customers in respect of whom Crown Melbourne or Crown Perth had formed suspicions. Some customers were

connected to former Crown Melbourne or Crown Perth customers who had been banned from those properties;

- d. many engaged in transfers of large values to or from other Crown Melbourne or Crown Perth customers in circumstances where Crown Melbourne or Crown Perth were not aware of, or did not understand, the connection between those customers;
 - e. many engaged in large financial transactions with unknown domestic or international third parties, including foreign remittance services;
 - f. many engaged in transactions indicative of known ML/TF typologies and vulnerabilities including structuring, offsetting, cuckoo smurfing, cashing-in large value chips with no evidence of play, and quick turnover of funds without betting;
 - g. many engaged in large cash transactions and transacted with cash that appeared suspicious, including cash in plastic bags, shoeboxes or cardboard boxes, cash in rubber bands, small denominations of notes and counterfeit cash;
 - h. Crown Melbourne and Crown Perth received numerous law enforcement requests with respect to some customers, some of which related to money laundering investigations and some of which related to conduct that had occurred at a Crown property;
 - i. Crown Melbourne and Crown Perth submitted numerous SMRs which reported repeated unusual or suspicious activity;
 - j. Crown Melbourne and Crown Perth were aware that some of the customers had been charged or arrested in connection with offences, including dealing with the proceeds of crime and money laundering; and
 - k. Crown Melbourne and Crown Perth were aware of information suggesting that some customers were connected to organised crime or that their source of funds/wealth may otherwise not be legitimate.
50. Despite these ML/TF risks, Crown Melbourne and Crown Perth continued to provide designated services to these customers, without carrying out appropriate risk-based ongoing due diligence, including enhanced customer due diligence. From 1 March 2016, these customers were either:
- a. not appropriately escalated to senior management in response to emerging ML/TF risks to determine whether an ongoing business relationship was within ML/TF risk appetite; or
 - b. if senior management did consider the ongoing business relationship, appropriate regard was not had to the ML/TF risks.
51. On and from 1 March 2016, designated services provided to these customers involved a turnover¹ by these customers in excess of \$70 billion and losses by these customers (or Crown wins) of about \$1.1 billion.
52. As some of these 60 customers were customers of both Crown Melbourne and Crown Perth, they account for 83 contraventions in total.

¹ In the casino context, turnover means the total amount wagered including any re-invested winnings.

The 447 customers engaging in repeated patterns of transactions consistent with ML/TF typologies - 464 contraventions

53. 447 customers of Crown Melbourne and Crown Perth engaged in transactions identified retrospectively by Crown's external consultants as being indicative of ML/TF typologies, including repeated patterns of:
- a. structuring;
 - b. cuckoo smurfing;
 - c. smurfing;
 - d. chip or casino value instruments cashing with minimal or no gaming activity; and/or
 - e. quick turnover of chips or casino value instruments with minimal or no gaming activity.
54. Had Crown Melbourne and Crown Perth been applying appropriate risk-based transaction monitoring, this suspicious activity could have been identified sooner.
55. Crown Melbourne's and Crown Perth's ability to fully understand who their customers were and to understand whether their transactions were legitimate was significantly limited by the:
- a. complexity and volume of customer transactions, including cross-border transactions;
 - b. inconsistent, conflicting or inaccessible customer identity information held within information management systems;
 - c. absence of source of funds and source of wealth information; and
 - d. involvement of third parties in the transfer of funds on behalf of customers.
56. These factors, combined with an absence of appropriate risk-based processes for transaction monitoring and enhanced customer due diligence, meant that Crown Melbourne and Crown Perth were unable to detect and appropriately manage customers whose transactional activity was highly indicative of ML/TF risks and typologies. These failures exposed Crown Melbourne and Crown Perth to the risk of being exploited by organised crime.
57. As some of these 447 customers were customers of both Crown Melbourne and Crown Perth, they account for 464 contraventions in total.

B. THE RELIEF SOUGHT FROM THE COURT

58. The Applicant seeks the following relief from the Court:
- a. declaratory relief under s 21 of the *Federal Court of Australia Act 1976* (Cth);
 - b. orders for civil pecuniary penalties under s 175 of the Act; and
 - c. costs.

C. THE PRIMARY LEGAL GROUNDS FOR THE RELIEF SOUGHT

59. Crown Melbourne and Crown Perth have each contravened s81 of the Act on an innumerable number of occasions on and from 1 March 2016.
60. Crown Melbourne has contravened s36 of the Act on 382 occasions in the period on and from 1 March 2016. Crown Perth has contravened s36 of the Act on 165 occasions in the period on and from 1 March 2016.
61. Each contravention attracts a maximum civil penalty between \$18 million and \$22.2 million.

D. THE ALLEGED HARM SUFFERED

62. Crown Melbourne and Crown Perth operate in an industry known, internationally and within Australia, to pose high ML/TF risks. The Crown Melbourne and Crown Perth Boards and senior management failed to adopt and maintain Programs to control those ML/TF risks appropriately. The casinos accordingly facilitated the provision of designated services in the billions of dollars in the absence of appropriate ML/TF controls.
63. Crown Melbourne and Crown Perth facilitated the movement of money into and out of the casino environment by way of designated remittance services. By facilitating this movement of money without appropriate AML/CTF controls, Crown Melbourne and Crown Perth exposed their banking partners and other financial institutions in transaction chains to ML/TF risks.
64. As a result of Crown Melbourne's and Crown Perth's non-compliance, the Australian and global community and financial system has been exposed to systemic ML/TF risks over many years. It is likely that many ML/TF risks were realised and that Crown Melbourne and Crown Perth were at risk of being exploited by organised crime.
65. In the absence of appropriate ML/TF risk oversight, a number of high risk practices, channels and customer relationships evolved. This permitted customers to move money through designated services in ways that involved ML/TF risks over and above those set out at paragraph 1. For example:
 - a. Crown Melbourne and Crown Perth used bank accounts in the names of shell companies (Southbank and Riverbank) to accept customer deposits. Warnings by banking partners that transactions on these accounts were indicative of money laundering were ignored and not escalated. Where accounts were closed because they were outside the banks' risk appetite, Crown Melbourne and Crown Perth opened new ones in their place.
 - b. Overseas deposit services were established in Manila and Macau with another casino, and in South East Asia with a remitter. These services permitted third parties not identified by Crown Melbourne or Crown Perth to deposit funds offshore that were then made available to Crown customers in Australia either by way of loans and/or remittance. These services were used by high risk junket operators and international VIPs, often in ways that were indicative of ML/TF typologies.
 - c. In May 2017, a Crown Resorts employee opened an account in his personal name with the Suncity junket in Macau. This account was intended to be a deposit service for debt repayments to Crown Melbourne, Crown Perth and Crown Aspinalls in London. Shortly after the Suncity deposit service arrangements were put in place, the decision to offer this deposit service was revisited due to 'local AML concerns' identified by Crown senior management. However, in May 2018, after the decision was made to discontinue the service, funds were remitted by Crown Melbourne via this channel on behalf of a customer who had been excluded from the casino as a result of criminal activity and concerns over source of wealth. By June 2018, senior management was advised there was still about \$25 million in the account.
 - d. On 27 March 2018, the VIP International team in Crown Resorts proposed that customer deposits at the Suncity desk in Macau would be transferred to Crown in Australia using the services of the remitter based in South East Asia who was operating a non-transparent deposit service. When the Suncity deposit service was not taken forward, the funds were returned to the original depositors, after which time the services of the remitter were used to remit some of the funds from the original depositors to either Crown Melbourne or Crown Perth. Whilst the ML/TF risks in relation to the Suncity deposit service were belatedly

recognised by Crown Melbourne and Crown Perth, the same ML/TF risks posed by the South East Asian remitter were not.

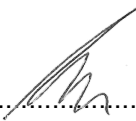
- e. Until October 2016, Crown Melbourne had a practice of receiving money at Crown Towers Hotel Melbourne from international VIP customers through the customer's credit or debit card, which was then made available to the customer for gaming at the casino. This channel lacked transparency and involved risks of capital flight. This practice was discontinued only after Crown staff were arrested in China.
 - f. Some junket operators were permitted to operate cash administration desks in private gaming rooms at Crown Melbourne and Crown Perth. Some junket operators were given access to a villa in Crown Towers Melbourne. Crown Melbourne does not know whether designated services were provided through those villas. Some junket operators were given access to the Crown private jet, on which large amounts of cash were carried into Australia. Some of these junket operators and their representatives were known to have connections to organised crime.
66. Appropriate controls were not in place to enable Crown Melbourne or Crown Perth to understand the sources of money moving through these high risk channels, or whether there was a risk that money was illicit. These business practices and risk management failures exposed Crown Melbourne and Crown Perth to the risk of money laundering. Crown Melbourne and Crown Perth chose to elevate their customers' desire for privacy over AML/CTF compliance, including in cases where Crown Melbourne or Crown Perth were aware customers had raised red flags.
67. In the absence of appropriate ML/TF controls, Crown Melbourne and Crown Perth facilitated the movement of significant amounts of money through high risk and non-transparent channels. A significant number of these transactions were also indicative of ML/TF typologies or vulnerabilities. By way of example, on and from 1 March 2016:
- a. Over \$300 million was transacted through Crown Patron accounts, including the Southbank and Riverbank accounts, involving transactions indicative of ML/TF typologies, exposing Crown Melbourne and Crown Perth to the risk of being exploited by organised crime.
 - b. About \$50 million was deposited through the Hotel Card Transaction channel by Crown Melbourne from 1 March 2016 to October 2016.
 - c. In May 2018, Crown Melbourne remitted \$4.8 million through the Suncity deposit service channel to settle a \$9.6 million debt owed to Crown by a former customer, who had been excluded from the casino 8 years earlier as a result of criminal activity and concerns over source of wealth.
 - d. From October 2016 to December 2018, there were at least 75 suspicious incidents involving cash in a private gaming room in Crown Melbourne to which one junket operator was given exclusive access. Cash in excess of \$23.5 million was involved, in circumstances where the identity of some of the persons presenting and removing the cash from the casino premises was and remains unknown.
68. On and from 1 March 2016, Crown Melbourne and Crown Perth provided designated services to 60 high risk customers, without carrying out appropriate risk-based due diligence. During this period, turnover by these customers was in excess of \$70 billion and losses by these customers (or Crown wins) was about \$1.1 billion. Crown Melbourne and Crown Perth chose to continue business relationships with these high risk customers, including high value customers with reported links to organised crime.

69. The non-transparent movement of money and deficiencies in KYC records inhibit the ability of law enforcement and AUSTRAC to trace money to its source. This inhibits law enforcement investigations, prosecutions and the recovery of proceeds of crime. Where money can be moved quickly and across borders, it can be even more difficult to trace and recover. These issues were compounded by Crown Melbourne's and Crown Perth's failures to ensure appropriate systems and controls to fully and accurately report SMRs, TTRs and IFTIs. Crown Melbourne's and Crown Perth's conduct has undermined the objectives of the Act.
70. The ML/TF risk management failures occurred in circumstances where Crown Melbourne and Crown Perth were operating a highly profitable business. Between July 2015 and June 2020, Crown Melbourne made over \$1 billion in revenue from junkets. Crown Perth's revenue from junket operations from 1 March 2016 was in excess of \$320 million. By failing to comply with the Act and Rules, Crown Melbourne and Crown Perth avoided expending funds that should have been invested in compliance including on IT, staffing and the development of AML/CTF controls. The money saved by Crown Melbourne and Crown Perth by its non-compliance is reflected in the scale of the expenditure on the current uplift of controls.

CERTIFICATE OF LAWYER

I, Sonja Marsic, certify to the Court that, in relation to the concise statement filed on behalf of the Applicant, the factual and legal material available to me at present provides a proper basis for each allegation in the pleading.

Date: 1 March 2022


.....

Sonja Marsic
AGS Lawyer
for and on behalf of the Australian Government Solicitor
Lawyer for the Applicant