IN THE HIGH COURT OF NEW ZEALAND
CHRISTCHURCH REGISTRY

I TE KŌTI MATUA O AOTEAROA
ŌTAUTAHI ROHE

CIV-2024-409-685
[2025] NZHC 2933

	BETWEEN	DEPARTMENT OF INTERNAL AFFAIRS Plaintiff
	AND	CHRISTCHURCH CASINOS LIMITED Defendant

Hearing: 18 September 2025

Appearances: S S McMullan and M Djurich for Plaintiff
G T Carter for Defendant

Judgment: 6 October 2025

JUDGMENT OF DUNNINGHAM J

This judgment was delivered by me on 6 October 2025 at 1.45 pm, pursuant to r 11.5 of the High Court Rules

Registrar/Deputy Registrar
Date:

Introduction

[1] Christchurch Casinos Ltd (CCL) operates a casino in Victoria Street, Christchurch. It is subject to various obligations under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (the Act). The Department of Internal Affairs (the Department), is the supervisor responsible for monitoring and enforcing CCL's compliance with the Act.[1]

[2] The Department has filed this civil proceeding against CCL, alleging breaches of the Act and seeking the imposition of pecuniary penalties. CCL has admitted that it has not complied with various obligations under the Act and has engaged with the Department to resolve the matter. That led to the parties entering into a settlement agreement. As a consequence of that agreement, the Department filed an amended statement of claim dated 31 July 2025 and CCL filed a notice of admissions dated 1 August 2025, admitting seven breaches of the Act.

[3] As part of the settlement, the parties agreed to jointly approach the Court to seek the imposition of a pecuniary penalty at an agreed level. The parties agree that CCL should be ordered to pay a penalty of $5,060,000 in respect of CCL's admitted breaches of the Act and have filed submissions in support of that outcome. In those circumstances it is accepted that the Court's role is not to embark on its own enquiry of what would be an appropriate penalty, but rather to consider whether the proposed penalty is within the proper range.[2]

CCL's business and AML/CFT obligations

[4] CCL owns and operates Christchurch Casino, New Zealand's first casino, having opened in 1984. As the holder of a casino operator's licence, CCL is a reporting entity under the Act[3] and its operations are subject to various obligations under the Act for the purpose of detecting and deterring money laundering and the financing of terrorism (ML/TF). This is in recognition of the fact that casinos have been assessed as having an overall "high" or "medium-high" ML/TF risk, and particular aspects of

---

1 Pursuant to s 130 of the Act.

2 *Financial Markets Authority v ANZ Bank New Zealand Ltd* [2021] NZHC 399 [ANZ] at [32]; and *Commerce Commission v Kuehne + Nagel International AG* [2014] NZHC 705 at [22].

3 As defined in s 5.

their business (cash transactions and junkets)[4] are assessed as presenting a high ML/TF risk.

[5] The obligations the Act imposes on a reporting entity such as CCL include establishing an anti-money laundering and countering the financing of terrorism (ML/CFT) compliance programme, undertaking transaction monitoring, conducting customer due diligence and enhanced customer due diligence when required, terminating business relationships when the requisite due diligence could not be undertaken and keeping records of transactions.[5]

[6] Over the period which is the subject of these proceedings (being 9 December 2018 to 8 December 2023), and as required by the Act,[6] CCL engaged two accounting firms, Crowe and BDO, to undertake independent audits of its risk assessment and AML/CFT programme. These reports raised a number of issues about CCL's compliance, although the earlier reports did not alert CCL to the fact it was in breach of the Act. The 2019 and 2021 independent reports recommended that CCL update its AML/CFT programme and should further automate its electronic monitoring system to reduce error rates arising from manual data entry. However, the 2024 independent audit report identified that CCL failed on a number of occasions to adhere to customer due diligence and prescribed transaction reporting requirements under the Act. Furthermore, CCL had not conducted a six-monthly internal AML audit during the audit period as specified in its AML/CFT programme.

[7] Importantly, in April 2021, the Department undertook an on-site inspection of CCL and identified some deficiencies in CCL's approach to customer due diligence and account monitoring. In its report of May 2021, the Department notified CCL of these deficiencies and required it to remediate them. CCL did not do so. Instead, it disputed the non-compliance findings and did not comply with the direction to remediate the non-compliances in a number of respects.

---

4 Which were explained during the hearing to be when commissions are paid to individuals to bring customers in from overseas.

5 As summarised in *Department of Internal Affairs v Ping An Finance (Group) New Zealand Company Ltd* [2017] NZHC 2363, [2018] 2 NZLR 552 *[Ping An]*.

6 Section 59.

[8] In May 2023 the Department commenced an investigation into CCL's compliance with the Act. Over the course of a year it issued seven notices requiring CCL to provide information and provide records. CCL accepts that there was some initial tardiness by it in responding to those notices. The Department's investigation included an assessment of compliance in relation to a sample of Players Club customers (the sample customers). Players Club members could, by moving up a membership tier, engage in cashless gambling at the casino. From 29 November 2021 CCL was required to undertake enhanced customer due diligence when a Players Club member upgraded their membership tier.

CCL's obligations under the Act

[9] CCL has a number of obligations under the Act and it is breaches of the following obligations which underpin these proceedings.

Requirement to establish implement and maintain an AML/CFT programme

[10] The Act requires reporting entities such as CCL to establish, implement and maintain an AML/CFT programme which includes internal procedures, policies and controls to detect money laundering and the financing of terrorism and to manage and mitigate the risk of these activities.[7] A reporting entity's AML/CFT programme must include adequate and effective procedures, policies and controls for, among other things, complying with customer due diligence requirements, keeping records, and monitoring and managing compliance with its procedures.[8]

Requirement to conduct account monitoring

[11] Reporting entities must also monitor customers' accounts and review their account activity.[9] They must ensure the information their customers provide initially, continues to match their activities and transaction behaviour, having regard to the level of risk posed by each customer.[10] Reporting entities must also ensure they have

---

7 Section 56(1).
8 Section 57(1).
9 Section 31.
10 Section 31(2)(a).

systems in place to identify transactions, or patterns of transactions, that raise a suspicion of ML/TF.[11]

Requirement to conduct customer due diligence

[12] A reporting entity is required to conduct customer due diligence if it establishes a business relationship with that customer or if a customer seeks to conduct an "occasional transaction" through that entity.[12]

[13] The level of due diligence required depends on the risk presented by the individual customer or transaction. At a minimum, reporting entities such as CCL must undertake standard customer due diligence which requires them to obtain verified information relating to the customer's identity,[13] the nature and purpose of their business relationship[14] and sufficient information to determine whether the customer should be subject to enhanced customer due diligence.[15]

[14] Enhanced customer due diligence requires, in addition to the standard customer due diligence requirements, obtaining verified information relating to the source of a customer's funds or wealth.[16] This enables the reporting entity to decide whether the funds used in a transaction are from legitimate sources.

Requirement to terminate existing business relationship

[15] Where adequate customer due diligence cannot be completed, there is a prohibition on establishing or continuing a business relationship with that customer or carrying out occasional transactions for the customer.[17]

---

11 Section 31(2)(b).
12 Section 14.
13 Sections 15 and 16(1)(b).
14 Section 17(a).
15 Section 17(b).
16 Sections 23(1)(a) and 24(1).
17 Section 37(1).

Requirement to keep records

[16] The Act prescribes the way in which reporting entities are required to maintain records obtained for the purpose of complying with the Act. These requirements are set out in subpart 3 of part 2 of the Act. As Toogood J held in *Ping An*:[18]

> Record keeping is the primary means by which the [supervisor] can supervise a reporting entity's compliance with the Act. Not keeping records makes it difficult sometimes impossible, to reconstruct transactions. This disrupts the ability to discern problematic patterns of transactions.

[17] This Court has interpreted the obligation to keep records as requiring the records to be kept in "such a way as to enable them to be viewed either immediately or upon request".[19] This is because "Any other interpretation would severely hamper the [supervisor's] ability to monitor compliance with other aspects of the regime.[20]

The admitted breaches

[18] CCL has admitted that it did not fully comply with its obligations under the Act in the relevant period. In particular, CCL accepts that it failed to:

(a) establish, implement and maintain a fully compliant AML/CFT programme in relation to compliance with customer due diligence requirements and in determining when enhanced customer due diligence was required;

(b) establish, implement and maintain a compliant AML/CFT programme in relation to record keeping (specifically, to keep written findings in respect of certain matters);

(c) establish, implement and maintain a compliant AML/CFT programme in relation to account monitoring and managing compliance;

(d) conduct adequate account monitoring;

---

18 *Ping An*, above n 5, at [107(b)].
19 *Department of Internal Affairs v OTT Trading Group Ltd* [2020] NZHC 1663 *[OTT]* at [76].
20 At [78].

(e) conduct compliant enhanced customer due diligence in respect of 24 customers;

(f) terminate existing business relationships in relation to these customers when it was required to do so; and

(g) keep records in accordance with the requirements of the Act.

[19] Having admitted those breaches the parties have conferred and reached agreement on the appropriate pecuniary penalties to be imposed in each case, supported by reference to case law.

Approach to pecuniary penalty

[20] While the Act creates a regime of civil, rather than criminal liability, the approach to imposing pecuniary penalties follows an analogous structure to the approach for criminal sentencing. It involves the following steps:[21]

(a) assessing the seriousness of the civil liability acts in order to set a starting point based on the seriousness of the non-compliance, by reference to the mandatory considerations listed in s 90 of the Act, and the aggravating and mitigating factors relating to it;

(b) considering aggravating and mitigating factors relating to the reporting entity, in order to determine whether these warrant the imposition of a higher or lower penalty;

(c) deducting from the starting point to reflect any admission of liability or co-operation with the authorities; and

(d) stepping back after steps (a) to (c) and undertaking a totality assessment by looking at each breach to ensure there is no overlap between the penalties imposed for different types of non-compliance, and

---

21 *Ping An*, above n 5, at [88].

considering whether the total penalty fairly and adequately reflects the overall extent of non-compliance.

[21] Using that framework, I go on to consider the parties' submissions on penalty having regard to the particular circumstances of this case, and in light of comparable case law.

Starting point

[22] As already noted, the starting point adopted for each civil liability act should reflect the gravity of the non-compliance with reference to the maximum penalty available under the Act and the mandatory considerations identified in s 90 of the Act.

[23] The maximum penalties prescribed by the Act for the civil liability acts admitted by CCL are, for failing to:

(a) conduct customer due diligence: $2 million;[22]

(b) adequately monitor accounts and transactions: $1 million;[23]

(c) terminate existing business relationships when required to by the Act: $1 million;[24]

(d) keep records in accordance with the requirements of subpart 3 of Part 2 of the Act: $2 million;[25] and

(e) establish, implement, and maintain an AML/CFT programme: $2 million (each).[26]

[24] The total maximum penalty CCL faces in respect of these civil liability acts is therefore $12 million.

---

22 Sections 78(a) and 90(3)(b).
23 Sections 78(b) and 90(2)(b).
24 Sections 78(c) and 90(2)(b).
25 Sections 78(e) and 90(3)(b).
26 Sections 78(f) and 90(3)(b).

[25] The starting points agreed by the parties are as follows:

(a) failing to establish, implement, and maintain an AML/CFT programme (relating to customer due diligence): $1,400,000

(b) failing to establish, implement, and maintain an AML/CFT programme (relating to record keeping): $1,200,000

(c) failing to establish, implement, and maintain an AML/CFT programme (relating to monitoring and managing compliance): $1,375,000

(d) failing to undertake adequate account monitoring: $850,000

(e) failing to conduct enhanced customer due diligence: $900,000

(f) failing to terminate existing business relationships: $150,000

(g) failing to keep records in accordance with the requirements of subpart 3 of Part 2 of the Act: $450,000

Total $6,325,000

[26] As already noted, my role in these circumstances is to consider whether the proposed penalty is "within the proper range".[27]

First cause of action: failing to establish, implement, and maintain a programme (relating to customer due diligence)

[27] The Department submits, and CCL acknowledges, that CCL operated in (and knew it operated in) a relatively high AML/CFT risk environment. The parties also accept that a key means of mitigating that AML/CFT risk is customer due diligence and that includes having the sufficient procedures, policies and controls in place to decide when enhanced customer due diligence is required.

---

[27] *Financial Markets Authority v Tiger Brokers (NZ) Ltd* [2023] NZHC 1625 *[Tiger]* at [36].

[28] From at least the start of the relevant period, CCL's AML/CFT programme was deficient in a number of respects as far as customer due diligence is concerned. These deficiencies included that CCL's AML/CFT programme allowed it, when it believed the customer was acting on behalf a third party, to proceed with a transaction even if a third party's identity could not be verified, provided there was approval to do so by an operation shift manager. The programme did not require CCL to verify whether the customer had the requisite authority to act on behalf of a third party. Furthermore, CCL's AML/CFT programme provided that enhanced customer due diligence had to be undertaken "where possible", rather than making it mandatory as required under s 22A of the Act. In addition, prior to September 2024, CCL's AML/CFT programme allowed the requirement to be satisfied of the source of a customer's funds when undertaking enhanced customer due diligence, to be met by asking a customer for their occupation, which did not meet the requirements of the Act.

[29] CCL's AML/CFT programme did not include any procedures, policies and controls relating to the following practices:

(a) Prior to September 2024 the programme did not provide any guidance on the circumstances which triggered the need for enhanced customer due diligence;

(b) Even after CCL ceased permitting junkets in February 2021, it still permitted some customers to introduce it to international customers in return for benefits paid for by CCL, such as flights, accommodation and other expenses, and to transact with CCL in a private capacity without meeting the criteria that formerly applied to junket participants. There were no procedures, policies and controls in CCL's AML/CFT programme to mitigate the risks associated with such transactions.

[30] In addition, from 29 November 2021, CCL implemented a "standard operating procedure" (SOP) which addressed, among other things, enhanced customer due diligence. However, the SOP included practices which were incorrect such as that enhanced customer due diligence "may" require the customer to declare their source of funds or source of wealth "if deemed necessary", which did not comply with the

Act. Furthermore, prior to the introduction of the SOP, CCL's AML/CFT programme did not provide for transaction value thresholds for the purpose of identifying whether enhanced customer due diligence ought to be conducted and this meant that CCL was unable to effectively determine whether a particular transaction was unusually large, such that enhanced customer due diligence was required.

[31] The Department also points out that CCL did not remediate the deficiencies identified in the 2021 on-site inspection report including the identified AML/CFT programme failures, and even when it took steps to address some of the issues raised by the Department, such as by implementing the SOP, non-compliances persisted.

[32] In setting the starting point, the parties agree that the closest comparators to the present case are *Reserve Bank of New Zealand v TSB Bank Ltd*[28] and *Department of Internal Affairs v SkyCity Casino Management Ltd*.[29]

[33] In *TSB*, the bank's AML/CFT programme did not contain adequate and effective documented assurance measures as required by s 57(1)(l) of the Act, for a period of six years, despite being advised of this deficiency by the Reserve Bank following its independent audits. The Court adopted a starting point for this breach of $1.25 million noting the length of time the deficiencies occurred over and the fact that, as a registered bank, TSB had a more central role in New Zealand's financial system compared with other reporting entities.

[34] In *SkyCity*, the casino's AML/CFT programme, like CCL's, included enhanced customer due diligence practices that were contrary to the Act and did not contain transaction value thresholds which identified when enhanced customer due diligence should be undertaken. However, SkyCity also had other deficiencies and, as a result of them, SkyCity customers engaged in just over $1 billion in transactions that should have been subject to enhanced customer due diligence but were not. Like CCL, SkyCity was made aware of some of its failures but did not immediately remediate them. For this breach, which spanned just over three years, this Court adopted a

---

28 *Reserve Bank of New Zealand v TSB Bank Ltd* [2021] NZHC 2241 *[TSB]*.
29 *Department of Internal Affairs v SkyCity Casino Management Ltd* [2024] NZHC 2781 *[SkyCity]*.

starting point of $1.5 million which Campbell J considered to be at the bottom of the available range.[30]

[35] The parties submit, and I agree, that CCL's conduct is more serious than that in *TSB*. Although the contraventions spanned a similar period, the consequences of CCL's breach were greater. It meant transactions of a significant value, which should have been subject to enhanced customer due diligence, were not, and prescribed transaction and suspicious activity reports were filed late or, on two occasions, not at all. CCL's relative size to TSB's is important. During the relevant period in *TSB*, the bank's annual revenue ranged from $124.6 million to $164.5 million. The gross value of CCL's total annual transactions for the relevant period range from $65.5 million to $377.3 million and, of these transactions, approximately 70 per cent were in cash, thus the ML/TF risk posed by CCL's transactions was greater than TSB's.

[36] I accept, though, that CCL's conduct is less serious than in *SkyCity* because SkyCity's AML/CFT programme-related breach related to several facets of its business, rather than customer due diligence alone, and the consequences in that case were greater. That said, I accept that the SkyCity breach involved a substantially shorter period than in the present case. Accordingly, the starting point proposed by the parties of $1.4 million, being 70 per cent of the maximum available, is appropriate.

Second cause of action: failing to establish, implement, and maintain a programme (relating to record keeping)

[37] The second cause of action is independent of the first cause of action and claims that during the relevant period, CCL's AML/CFT programme was deficient in so far as its record keeping obligations were concerned.

[38] CCL's AML/CFT programme provided that it would maintain account monitoring records on an exceptions basis, which meant that only variances or exceptions that required further investigation would be recorded. It also provided that CCL would keep written findings in respect of a number of other matters. However, despite that, CCL failed to implement some of its own required record keeping

30 At [64].

procedures, policies and controls. In particular, it did not keep written findings in respect of the following:

(a) any exception-based account monitoring;

(b) where a person was deemed to be a person of interest by CCL's surveillance department, the reason for this categorisation; and

(c) the investigation of potentially suspicious activities.

[39] As a result of these failures, CCL did not keep all records it was required to under subpart 2 of Part 3 of the Act. It was unable to provide all documents, records or information in response to three statutory notices issued by the Department. It also could not comply with the timeframes to respond to two of the notices and, because of this, the Department was unable to readily reconstruct the transactions that it sought from CCL.

[40] None of the pecuniary penalty cases decided under the Act have involved cause of action relating to deficient record keeping practices under an AML/CFT programme. As there is no comparator case or guideline judgment, the appropriate penalty range must be ascertained from the seriousness of the breach and the maximum penalty. In that regard, some assistance can be drawn from *Financial Markets Authority v ANZ Bank Ltd*, where Muir J reviewed the pecuniary penalty decisions made under the Act and attempted to identify bands for the level of penalty imposed by descriptors of the conduct. Specifically, he summarised the following level of penalty observed in decided cases:[31]

(a) between 50 and 70 per cent of the available maximum for conduct involving:

(i) "serious, systemic deficiencies in complying with a multiplicity of obligations under the Act" in circumstances showing a disregard of the Act's requirements;

(ii) long-term non-compliance with the Act, despite prior oversight and warnings from the [AML/CFT supervisor] and

---

31 *ANZ*, above n 2, at [80] (footnotes omitted).

despite the company having had ample evidence that the transactions processed were suspicious;

(iii) "brazen" contraventions of the enhanced due diligence requirements occurring across a significant volume of transactions.

(b) between 25 and 33 per cent of the available maximum for conduct involving significant contraventions, but in circumstances which suggest that the defendant had made at least some attempt to comply with their obligations; and

(c) between six and 11 per cent of the available maximum for conduct involving inadvertent breaches by a company which was unaware that it was substantially non-compliant.

[41] While both parties submitted that this summary of penalty orders needed to be treated with some caution, they also acknowledged that several cases had considered Muir J's summary a "helpful cross-check in relation to totality".[32]

[42] In the present case, the parties propose a penalty of $1.2 million, being 60 per cent of the available maximum. In setting this starting point, they note that CCL's failure to implement some of its record keeping practices was systemic and occurred over a long period of time, but it was not a case where the programme did not provide for record keeping, or where no record keeping practices were implemented.

[43] In my view, this fairly reflects the extent of the breach, being a systemic deficiency over an extended period of time, albeit not the most serious or flagrant type of contravention, noting it is clear that reports of suspicious transactions were kept. Accordingly, I accept the penalty of $1.2 million is within range.

Third cause of action: failing to monitor and manage compliance of AML/CFT programme

[44] Throughout the relevant period, CCL's AML/CFT programme provided that there would be internal audits completed quarterly before February 2021 and thereafter bi-annually, and that the programme would be reviewed and if necessary updated at least once every 12 months.

---

32 *Tiger*, above n 27, at [34].

[45] Despite this, CCL:

(a) ceased conducting internal AML audits after September 2020;

(b) failed to review or revise its AML/CFT programme between June 2021 and September 2024; and

(c) put the revision of its AML/CFT programme on hold until the 2024 independent audit report and recommendations became available.

It did, however, implement and revise the SOP from November 2021 onwards.

[46] CCL was put on notice of the need to update its AML/CFT programme in the 2019, 2021 and 2024 independent audit reports. The Department notes that as a result of these failures, CCL was unable to identify the deficiencies noted in the Department's 2021 on-site inspection report or the matters and issues raised in the 2021 and 2024 independent audit reports.

[47] Both parties say that, in setting the starting point, the decision in *TSB* is the most analogous case. There, TSB failed to regularly review and maintain its AML/CFT programme over a period of approximately four years. This came to light because one of TSB's independent audits identified issues around staff training and transaction monitoring. However, by the time of the next independent audit, two years later, the identified issues remained unaddressed. The Court adopted a starting point of $1.375 million for this breach.

[48] Here, it is clear that CCL's failure to implement compliance related measures and to review its AML/CFT programme is at least as serious as TSB's breach. The failures to review and update the respective AML/CFT programmes occurred over a significant period of time, were contrary to internal review periods, and independent audits had identified the need for the programmes to be updated. Accordingly, the parties submit, and I agree, that the same starting point adopted in *TSB*, being $1.375 million, is the appropriate penalty for this failing.

Fourth cause of action: failing to conduct adequate account monitoring

[49] The Act requires a reporting entity to undertake ongoing account monitoring, including by regularly reviewing customer account activity and behaviour.[33] At all relevant times, CCL did have automated and manual account monitoring controls in place. From 2021, this included the automated Jade system which raised alerts in respect of transactional activity in accordance with rules set by CCL.

[50] However, each of CCL's account monitoring records had significant limitations, and the failure to undertake adequate account monitoring was demonstrated in respect of 24 of the 26 sample customers which the Department had sought transaction records for.

[51] CCL accepts that it failed to undertake adequate account monitoring in respect of those customers, and across its business more generally, saying it was because:

(a) Before the introduction of the Jade system, CCL relied on manual account monitoring to comply with its obligations under the Act and, in particular, an occasional transactions register. That occasional transaction register relied on the manual input of data and was susceptible to error.

(b) Both prior to and after the Jade system was implemented, large cash transactions were automatically identified for Players Club members, but these were also manually recorded in the occasional transaction register and therefore susceptible to error. The manual recording was necessary because the Jade system was unable to identify parts of transactions which were in cash. Similarly, international funds transfers required manual recording.

[52] That said, CCL accepts that its account monitoring systems overall were susceptible to error. By way of example, the Department identified, among other things:

---

[33] Section 31.

(a) 285 duplicate transactions;

(b) multiple transactions conducted by the same customer but where the customer's name or Players Club number differed across the customer's transactions; and

(c) over 2,000 transactions where information was recorded in the third party customer fields but of which only 599 actually recorded third party customer information and, for 143 of these, there was insufficient information to identify the third party.

[53] In terms of setting the starting point, the parties agree that the most analogous case is SkyCity. Despite having automated and manual account monitoring controls in place, including the Jade system, SkyCity failed to undertake adequate account monitoring, including because the Jade system still required additional manual account monitoring and SkyCity did not have sufficient resources in its AML/CFT team to do this. SkyCity's failure, which was identified in respect of 18 sample customers, was representative of the way in which it undertook account monitoring across its business over a five year period.

[54] In *SkyCity*, Campbell J adopted a starting point of $750,000 but here, CCL accepts that a higher starting point of $850,000 is appropriate. This is to reflect the fact that CCL's account monitoring breach was greater than that in *SkyCity*. First, for around half the relevant period, CCL did not use automated transaction monitoring rules for the predominant purpose of complying with its obligation under the Act. This differs from *SkyCity* where automatic monitoring systems were in place at all times and used for account monitoring purposes.

[55] Second, CCL's account monitoring processes were susceptible to error and CCL was alerted to this weakness in the 2019 independent audit report and again, in the Department's 2021 on-site inspection report. However, CCL's non-compliance persisted even after the Jade system was implemented in late 2021, as CCL still relied on manual input which was susceptible to error. Furthermore, the parties note that CCL's account monitoring breach meant it was unable to comply with its record

keeping obligations under subpart 3 of Part 2 of the Act, and therefore to provide the information sought through the Department's notices in a timely way, and this was a factor not present in *SkyCity*. The Department says that as a consequence, an unknown number of customers, including the 24 customers identified through its sample, should have been the subject of enhanced due diligence but were not. Furthermore, CCL was unable to identify all the transactions engaged in by the sample of customers which should have been the subject of a prescribed transaction report or suspicious activity report. CCL also failed to make, within the time specified under the Act, or in two incidences at all, such reports in respect of 150 prescribed and 12 suspicious transactions.

[56] For all these reasons, the parties propose a starting point of $850,000 out of the maximum penalty of $1 million. I consider this starting point is at the highest end of the available range, given:

(a) a key reason for the $750,000 penalty in *SkyCity* was the size of its business and therefore the extent of customers' transactions which were likely to have not been adequately monitored;[34] and

(b) the present case is not one where there were no account monitoring controls in place but rather where they were deficient.

[57] I nevertheless accept that the agreed penalty of $850,000 should not be disturbed.

Fifth cause of action: failing to conduct enhanced customer due diligence

[58] The Act requires CCL to carry out enhanced customer due diligence in a range of circumstances, including where a customer seeks to conduct a complex, unusually large transaction, or unusual pattern of transactions that have no apparent or visible economic or lawful purpose, where a suspicious activity report must be filed, or where a reporting entity considers that the level of risk involved is such that enhanced due diligent should apply to a particular situation.[35]

---

34 At [72].
35 Section 22(1)(a)–(e).

[59] Enhanced customer due diligence requires the verification of identity requirements and, according to the level of risk involved, reasonable steps being taken to verify source of funds or wealth.[36]

[60] CCL accepts that 24 of their sample customers engaged in transactions which triggered the requirement to undertake enhanced customer due diligence, but that it did not undertake the required level of due diligence. This was largely due to deficiencies in CCL's AML/CFT programme, which have already been discussed. As a consequence, transactions totalling approximately $56 million were undertaken with these customers after the date on which CCL ought to have undertaken compliant enhanced customer due diligence. The Department points out that several instances were particular egregious noting:

(a) 17 of the 24 sample customers engaged in transactions after the point in time when CCL was required to conduct enhanced customer due diligence on them;

(b) five of the sample customers were the subject of one or more suspicious activity reports which gave rise to the requirement to conduct enhanced customer due diligence on them;

(c) two of the sample customers were the subject of a suspicious activity report after the point in time when CCL was required to conduct enhanced customer due diligence on them;

(d) the transactional activity of 11 of the sample customers was sufficiently concerning to CCL that it resulted in a ban. Despite this, enhanced customer due diligence was still not conducted; and

(e) some of the customers engaged in significant transactions after the point in time when CCL was required to conduct enhanced customer due diligence on them.

---

36 Section 24(1).

[61] The parties are, however agreed that CCL's conduct is less serious than that in the majority of cases involving a failure to adequately conduct customer due diligence. For example, starting points of $1.3 million were adopted in *Ping An*, where there was a widespread failure to conduct compliant customer due diligence in respect of 362 customers, and other decisions (*Jin Yuan* and *OTT*) involved much larger value of transactions. Similarly, in *SkyCity* a starting point of $1.6 million was adopted in respect of transactions involving 18 customers and totalling just over $1.065 billion. The parties are agreed that the decisions in *CLSA* and *Tiger* are more comparable.[37]

[62] A starting point of $400,000 was adopted in *CLSA* in relation to 12 transactions undertaken by 10 customers, totalling $49.5 million and in *Tiger* a starting point of $550,000 was adopted in relation to 21 customers who undertook transactions totalling $56.5 million.

[63] Here, CCL's breach involved the 24 sample customers who undertook just under $56.2 million in transactions which should have been subject to enhanced customer due diligence checks but were not. Given CCL's failure to undertake compliant enhanced customer due diligence was more serious than that in *CLSA* and *Tiger*, because it occurred over a longer period, the parties propose, and I accept, that a starting point of $900,000 is appropriate.

Sixth cause of action: failing to terminate existing business relationships

[64] As a result of CCL's failure to conduct enhanced customer due diligence in respect of the 24 sample customers, there was a related requirement to terminate its business relationship with these customers. While CCL subsequently issued bans to 11 of these customers, the ban did not amount to a termination of the business relationship with the customers. Furthermore, before September 2024, CCL's AML/CFT programme did not address when it was required to terminate its business relationship with a customer.

---

[37] *Tiger*, above n 27, at [33]; and *Financial Markets Authority v CLSA Premium New Zealand Ltd* [2021] NZHC 2325; [2021] NZCCLR 16 [CLSA] at [51].

[65] As the Department notes, CCL's failure to terminate business relationships is directly linked to its conduct in failing to undertake compliant enhanced customer due diligence in respect of these customers. Given this breach is inextricably linked to the failure to carry out compliant enhanced customer due diligence when required, the parties note that care must be taken not to "double count" CCL's breaches. While, on a standalone basis, a starting point of between $400,000 and $500,000 would likely have been warranted, having regard to the principle of totality, the parties propose that a discrete penalty of $150,000 is appropriate.

[66] I accept here that the obligations to undertake enhanced customer due diligence and to terminate business relationships when the outcome of that due diligence process requires are, here, clearly inter-related. This is not a case where enhanced customer due diligence was carried out, but where, as a result of that, a requirement to terminate a business relationship was not actioned. Rather, the failure is a direct consequence of the deficiencies in conducting enhanced customer due diligence. For this reason, I accept that a relatively modest penalty of $150,000 is warranted. This reflects the approach adopted by Edwards J in *CLSA*, where she recognised that the obligation to terminate a relationship under s 37 was different from the obligation to obtain certain information through the customer due diligence requirements, but where she also recognised that where the failure under s 37 flows from the failure to conduct proper customer due diligence, a lower penalty is warranted than when this is standalone conduct.[38]

Seventh cause of action: failing to keep records in accordance with the requirements of subpart 3 of Part 2 of the Act

[67] The Act requires reporting entities to keep a range of records, including records that are reasonably necessary to enable a transaction to be readily reconstructed at any time, reports of suspicious activities, and identity and verification records. While CCL kept transaction records, reports of suspicious activities, and identity and verification records, there were systemic problems with its record keeping.

---

[38] *CLSA*, above n 37, at [57]–[60].

[68] As already noted, due to the way the account monitoring records were kept and the manual process required to identify and compile information, CCL had difficulty in responding to notices issued by the Department. CCL also omitted some information in records relating to the sample customers due to the manual process required to identify and compile the information the Department had requested. CCL accepted that the way it kept its records in respect of the sample customers was representative of its record keeping more generally.

[69] That said, the Department recognises that this cause of action overlaps with the second cause of action, which is based on a failure in the implementation of its AML/CFT programme in relation to record keeping. However, the scope of the failure identified in this cause of action is broader because it relates to CCL's ability to readily identify records to be provided to the Department to enable it to reconstruct transactions and monitor compliance. Consequently, it covers a broader set of conduct than simply record keeping pursuant to its AML/CFT programme.

[70] In setting the starting point, the parties note that CCL's breach falls somewhere between those identified in *OTT*, on the one hand, where a starting point of $500,000 was adopted for significant gaps in the organisation's records, and the starting points of $300,000 and $350,000 imposed in *Tiger Brokers* and *CLSA* respectively, with the parties saying this case is similar in that it involved an absence of some records and a concern with the way other records were kept. The primary differences are that CCL's breach took place over a longer time period, and the pleaded claim is representative in nature. Accordingly, the parties submit that a starting point of $450,000 is appropriate, placing it between the starting points adopted in the other cases discussed.

[71] I agree that a penalty in this order is within the range.

Aggravating and mitigating factors

[72] The parties are agreed there are no aggravating factors relating to CCL. In terms of mitigating factors, the parties agree that CCL is entitled to a deduction of 20 per cent from the starting point penalty in order to reflect its cooperation and relatively early admissions.

[73] The Department acknowledges that CCL engaged with it and sought to resolve the Department's allegations at a relatively early stage of the proceedings. This included reaching agreement on both the factual basis for the breaches, and on the appropriate penalty to be imposed.

[74] In *SkyCity* and *Tiger Brokers*, reductions of 25 per cent for early admission and cooperation were considered appropriate. In *TSB*, the parties had agreed that TSB's admission and cooperation entitled it to a reduction of 20 per cent. However, the Court concluded that this was unduly low and would "operate unfairly" on other defendants who admitted responsibility and fully cooperated, so the deduction was increased to 25 per cent.[39]

[75] In *CLSA* and *Department of Internal Affairs v Qian Duoduo Ltd*,[40] deductions of 23 and 20 per cent, respectively, were applied to reflect the defendants' admissions of liability and cooperation. In both cases, there was cooperation and the admissions occurred at an early stage, although, unlike CCL, the penalty was not agreed. Here, CCL accepts its admissions did not occur as soon as was the case in *SkyCity*, *Tiger Brokers*, and *TSB*. Nevertheless, it did cooperate reasonably promptly with the Department and therefore accepts that a 20 per cent reduction is appropriate.

[76] Acknowledging CCL's cooperation at a reasonably early stage, but not as soon as the deficiencies were identified, I agree a 20 per cent reduction is within the available range.

Totality

[77] Applying a 20 per cent reduction to the total penalty of $6.325 million results in a final penalty of $5.06 million. The parties are agreed that a final penalty pecuniary in that amount reflects the seriousness of CCL's civil liability and promotes the purpose of the Act. To the extent there is any overlap in the acts that form the breaches, that has been accounted for in the various starting points adopted and the parties are

---

39 *TSB*, above n 28, at [45].
40 *Department of Internal Affairs v Qian Duoduo Ltd* [2018] NZHC 1887.

agreed that there is no need to make further adjustments to the penalty to reflect totality considerations.

[78] Again, I see no reason to depart from the parties' conclusions. There were serious systemic deficiencies in CCL's systems and in its oversight of its operations. While the breaches of the Act were not necessarily deliberate, the failure to act promptly when alerted to the deficiencies can be criticised, as can the somewhat casual approach which was taken by CCL to the extremely important obligations it has under the Act to deter and prevent AML/CFT activities. The end penalty is significant. It reinforces the importance of strict adherence to the Act's requirements and, by doing so, achieves the purposes of the Act, including to detect and deter money laundering and the financing of terrorism, and to enhance confidence in New Zealand's financial system.[41]

Conclusion

[79] Accordingly:

(a) I enter judgment on the seven causes of action pleaded against CCL.

(b) CCL is ordered to pay a civil pecuniary penalty of $5.06 million.

(c) There is no order as to costs.

Solicitors:
MC, Auckland
Chapman Tripp, Christchurch

[41] Section 3.