[REDACTED FOR PUBLICATION]

**IN THE HIGH COURT OF NEW ZEALAND**
**AUCKLAND REGISTRY**

**I TE KŌTI MATUA O AOTEAROA**
**TĀMAKI MAKAURAU ROHE**

**CIV-2025-404-3682**
**[2026] NZHC 1537**

| | |
|---|---|
| BETWEEN | RESERVE BANK OF NEW ZEALAND<br>Plaintiff |
| AND | ASB BANK LIMITED<br>Defendant |

Hearing: 9 March 2026

Appearances: S S McMullan and M Djurich for Plaintiff
B A Keown and M C Staines for Defendant

Judgment: 3 June 2026

---

**JUDGMENT OF O'GORMAN J**

---

*This judgment was delivered by me on 3 June 2026 at 2 pm pursuant to r 11.5 of the High Court Rules 2016.*

*Registrar/Deputy Registrar*

……

Solicitors/Counsel:
Meredith Connell, Auckland
Bell Gully, Auckland

## Introduction

[1] This is a hearing to impose a civil pecuniary penalty on ASB Bank Ltd (ASB) for contravening its obligations under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (Act).

[2] The Act defines anti-money laundering and countering the financing of terrorism as "AML/CFT".[1] The Reserve Bank of New Zealand (Reserve Bank) is the AML/CFT supervisor responsible for monitoring and enforcing compliance with the Act by registered banks.[2]

[3] The parties agree and jointly submit that ASB should be ordered to pay a penalty of $6.731 million for various breaches of the Act. They consider such a penalty is appropriate as deterrence, to reflect the nature and duration of ASB's contraventions, and to recognise that ASB has accepted responsibility for the breaches early in these proceedings.

[4] I must determine whether the recommended penalty is appropriate (within range) considering the statutory criteria, relevant case law and the particular circumstances of ASB's conduct.

## Relevant legal principles

*Purposes of the Act*

[5] As described during its third reading, the Act is part of New Zealand's ongoing contribution to global efforts to combat money laundering and terrorist financing (ML/TF):[3]

> The passage of the bill into law will help to maintain New Zealand's international reputation and confidence in our financial trading system. Most of New Zealand's financial trading partners have already implemented robust anti-money-laundering and countering financing of terrorism regimes. In a global economy, countries and businesses are looking for stable, safe economies with which to do business. The passage of this bill into law will

1 Anti-Money Laundering and Countering Financing of Terrorism Act 2009, s 5.
2 Sections 5 and 130(1)(a).
3 (15 October 2009) 658 NZPD 7098. The Act is a successor to the Financial Transactions Reporting Act 1996.

> demonstrate New Zealand's commitment to assisting with what is an international problem. The legislation implements measures established by the Financial Action Task Force, which is an inter-Governmental body that sets international standards for combating money-laundering and terrorist financing.
>
> The bill anticipates a significant amount of cooperation between industry and Government to ensure that the regime is responsive to risk, and effective at detecting and deterring criminal activity. The bill, as far as possible, enables businesses to focus their resources on those customers or products that represent the most risk. However, to achieve the bill's aims, financial service providers and casinos will need to ensure they have appropriate customer due diligence measures and that they can identify and report suspicious activity. The framework the bill establishes is appropriate to New Zealand's financial system, and is aligned with the frameworks of our trading partners, particularly those of Australia.

[6] The purposes of the Act are:[4]

(a) to detect and deter money laundering and the financing of terrorism; and

(b) to maintain and enhance New Zealand's international reputation by adopting, where appropriate in the New Zealand context, recommendations issued by the Financial Action Task Force; and

(c) to contribute to public confidence in the financial system.

*Reporting entity obligations*

[7] To achieve the above purposes, Pt 2 of the Act imposes various obligations on reporting entities, including registered banks:[5]

(a) Subpt 1 includes provisions dealing with requirements on reporting entities to conduct due diligence on customers and certain other persons, the ability of reporting entities to rely on third parties to carry out customer due diligence and other AML/CFT functions, and

---

4 Anti-Money Laundering and Countering Financing of Terrorism Act, s 3(1).

5 Section 4(3). See also *Department of Internal Affairs v Ping An Finance (Group) New Zealand Co Ltd* [2017] NZHC 2363, [2018] 2 NZLR 552 at [21]; *Financial Markets Authority v CLSA Premium New Zealand Ltd* [2021] NZHC 2325, [2021] NZCCLR 16 at [21]; and *Financial Markets Authority v Tiger Brokers (NZ) Ltd* [2023] NZHC 1625 at [19].

prohibitions on establishing or continuing business relationships and setting up facilities in certain circumstances.

(b) Subpt 2 includes provisions requiring reporting entities to report suspicious activities (subpart 2A mandates reports for certain types of prescribed transactions).

(c) Subpt 3 sets out requirements on reporting entities to keep records and includes provisions concerning the storage and destruction of records.

(d) Subpt 4 includes provisions requiring reporting entities to have an AML/CFT programme for detecting and managing the risk of money laundering and the financing of terrorism, to carry out a risk assessment before conducting customer due diligence or establishing an AML/CFT programme, and to review, audit and report on their risk assessment and AML/CFT programmes.

[8] Under subpt 1 of pt 2, a reporting entity must conduct customer due diligence if the circumstances in ss 14, 18 or 22 of the Act apply. Subpt 1 contains a hierarchy of standards ranging from simplified due diligence to enhanced customer due diligence. The obligations require (at a minimum) verifying the customer's identity as prescribed,[6] and conducting enhanced customer due diligence (more wide-ranging verification obligations about beneficial interests and the source of a customer's funds or wealth) in a range of specified circumstances, including when the level of risk is such that enhanced due diligence should apply to a particular situation,[7] or when a suspicious activities report is required.[8]

[9] Under ss 37–39 of the Act, a reporting entity is prohibited from establishing or continuing a business relationship with a customer or carrying out an occasional transaction for a customer, where adequate customer due diligence cannot be

---

6 Anti-Money Laundering and Countering Financing of Terrorism Act, s 20.
7 Section 22(1)(d).
8 Section 22A.

completed. Where a business relationship has been established, this requires the reporting entity to terminate the relationship.[9]

[10] Under subpt 2 of pt 2 of the Act, reporting entities are required to report suspicious activity to the police,[10] so police can investigate potential money laundering and other crime. Suspicious activity is defined in s 39A. This arises in circumstances including when a person conducts or seeks to conduct a transaction through a reporting entity, and the reporting entity has reasonable grounds to suspect the transaction may be relevant to the investigation or prosecution of any person for money laundering, or for a criminal offence, or relevant to the enforcement of the Misuse of Drugs Act 1975, the Terrorism Suppression Act 2002, the Proceeds of Crime Act 1991, or the Criminal Proceeds (Recovery) Act 2009. The Act requires reports to be made within three working days of forming the requisite suspicion.[11] The short window reflects the Act's emphasis on early detection.[12]

*Reporting entity risk assessments*

[11] Section 58 of the Act requires a reporting entity to undertake a risk assessment before conducting due diligence or establishing an AML/CFT programme. The risk assessment must identify the risks faced by the reporting entity in the course of its business.[13] Such risk assessments are informed by sector risk assessment reports issued by the various AML/CFT supervisors referred to in s 130.

[12] The Reserve Bank's 2017 sector risk report for registered banks, life insurers and non-bank deposit takers classifies banks as being exposed to an inherently "high" risk of ML/TF because the value, volume and velocity of banking transactions provide an environment which can readily be used to conceal, disguise or obfuscate the

---

9 *Financial Markets Authority v Tiger Brokers (NZ) Ltd*, above n 5, at [23].

10 Under s 41(3) of the Anti-Money Laundering and Countering Financing of Terrorism Act, the report must be made to those police employees who have the Commissioner of Police's authority to receive such reports, which is the New Zealand Financial Intelligence Unit (FIU). The FIU has on online platform for making suspicious activity reports and has issued guidelines, available at www.police.govt.nz.

11 Anti-Money Laundering and Countering Financing of Terrorism Act, s 40(1).

12 *Department of Internal Affairs v Ping An Finance (Group) New Zealand Co Ltd,* above n 5, at [107(c)].

13 Anti-Money Laundering and Countering Financing of Terrorism Act, s 58(3)(a).

proceeds of crime.[14] The important part that registered banks play in the financial sector in New Zealand, coupled with the relative complexity of their products and business models and exposure to international financial systems, are the primary factors in the overall risk rating for banks.[15]

[13] By way of comparison, the risk report by the Department of Internal Affairs in 2019 covered casinos, trust and company service providers, high-value dealers, the Racing Industry Transition Agency and "designated non-financial businesses or professions"[16] (including lawyers, accountants, conveyancers, and real estate agents).[17] That report classified only trust and company services providers as having an inherently high risk of ML/TF, ranking those risks higher than other entity types including casinos (given a "medium-high" classification).[18]

*Civil penalty provisions*

[14] Section 78 of the Act provides that a failure to comply with AML/CFT requirements (including those set out in Pt 2) amounts to a "civil liability act" for the purposes of the Act's enforcement regime:

> **78 Meaning of civil liability act**
>
> In this Part, a civil liability act occurs when a reporting entity fails to comply with any of the AML/CFT requirements, including, without limitation, when the reporting entity—
>
> (a) fails to conduct customer due diligence as required by subpart 1 of Part 2:
>
> (b) fails to adequately monitor accounts and transactions:
>
> (c) enters into or continues a business relationship with a person who does not produce or provide satisfactory evidence of the person's identity:
>
> (d) enters into or continues a correspondent banking relationship with a shell bank:

---

14 Reserve Bank of New Zealand *Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) | Sector Risk Assessment for Registered Banks, Non-Bank Deposit Takers and Life Insurers* (April 2017), available at www.rbnz.govt.nz, at [57].

15 At [59].

16 Anti-Money Laundering and Countering Financing of Terrorism Act, ss 5, 6 and 130(1)(c).

17 Department of Internal Affairs *Designated Non-Financial Businesses and Professions (DNFBPs) and Casinos Sector Risk Assessment* (December 2019), available at www.dia.govt.nz.

18 At [15].

(da) fails to report transactions in accordance with subpart 2A of Part 2:

(e) fails to keep records in accordance with the requirements of subpart 3 of Part 2:

(f) fails to establish, implement, or maintain an AML/CFT programme:

(g) fails to ensure that its branches and subsidiaries comply with the relevant AML/CFT requirements:

(h) enters into cash transactions in relation to certain items in breach of section 67A.

[15] Under s 90(1) of the Act, on the application of the relevant AML/CFT supervisor, the High Court may order a person to pay a pecuniary penalty to the Crown, or to any other person specified by the Court, if the Court is satisfied that that person has engaged in conduct that constituted a civil liability act.

[16] Section 90(4) specifies the following mandatory considerations for the Court when determining an appropriate pecuniary penalty:

(a) the nature and extent of the civil liability act; and

(b) the likelihood, nature and extent of any damage to the integrity or reputation of New Zealand's financial system because of the civil liability act; and

(c) the circumstances in which the civil liability act occurred; and

(d) whether the person has previously been found by the Court in proceedings under the Act to have engaged in any similar conduct.

[17] The maximum amount of pecuniary penalty depends on which of two categories applies:

(a) the maximum is $1 million for a body corporate or partnership, or $100,000 for an individual, for the civil liability acts specified in s 78(b), (c), (d) or (g);[19]

[19] Anti-Money Laundering and Countering Financing of Terrorism Act, s 90(2).

(b) the maximum is $2 million for a body corporate or partnership, or $200,000 for an individual, for civil liability acts specified in s 78(a), (da), (e), (f) or (h).[20]

*Setting a penalty*

[18] A penalty under s 90 is set using a four-step framework:[21]

(a) *Starting point*: 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) *Aggravating and mitigating factors*: 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) *Admissions and cooperation*: deducting from the starting point to reflect any admission of liability or co-operation with the authorities.

(d) *Totality*: stepping back after steps (a)–(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 considering whether the total penalty fairly and adequately reflects the overall extent of non-compliance.

[19] In cases where the parties agree on a jointly proposed penalty, the Court's role is not to embark on its own enquiry of what is an appropriate penalty, but rather to

---

20 Section 90(3).

21 *Department of Internal Affairs v Ping An Finance (Group) New Zealand Co Ltd*, above n 5, at [88]; *Department of Internal Affairs v Qian Duoduo Ltd* [2018] NZHC 1887 at [25]; *Department of Internal Affairs v Jin Yuan Finance Ltd* [2019] NZHC 2510 at [27]; *Department of Internal Affairs v OTT Trading Group Ltd* [2020] NZHC 1663 at [51]; *Department of Internal Affairs v SkyCity Casino Management Ltd* [2024] NZHC 2781 at [22]; and *Department of Internal Affairs v Christchurch Casinos Ltd* [2025] NZHC 2933, [2025] NZCCLR 964 at [20].

consider whether the proposed penalty is within the proper range.[22] In so doing, the Court must satisfy itself that the proposed final figure satisfies the objectives of the Act and reflects the case's particular circumstances.[23] The Court takes a broader approach because there is a significant public benefit in promoting voluntary resolutions that avoid time-consuming and costly investigation and litigation.[24]

[20] In *Financial Markets Authority v ANZ Bank New Zealand Ltd*, Justice Muir analysed various cases imposing penalties under the Act as falling within the following ranges:[25]

(a) between 50 and 70 per cent of the available maximum for conduct involving serious, systemic deficiencies in complying with a multiplicity of obligations under the Act, long-term non-compliance with the Act despite warnings, or "brazen" contraventions of the enhanced due diligence requirements;

(b) between 25 and 33 per cent of the available maximum for conduct involving significant contraventions, but in circumstances suggesting that a 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 unaware that it was substantially noncompliant.

---

22 *Department of Internal Affairs v Christchurch Casinos Ltd*, above n 21, at [3]; *Financial Markets Authority v Tiger Brokers (NZ) Ltd*, above n 5, at [36]; and *Reserve Bank of New Zealand v TSB Bank Ltd* [2021] NZHC 2241, [2021] NZCCLR 27 at [3].

23 *Financial Markets Authority v ANZ Bank New Zealand Ltd* [2021] NZHC 399, (2021) 16 TCLR 28 at [32]; *Department of Internal Affairs v SkyCity Casino Management Ltd*, above n 21, at [28]–[29].

24 *Department of Internal Affairs v SkyCity Casino Management Ltd*, above n 21, at [29].

25 *Financial Markets Authority v ANZ Bank New Zealand Ltd*, above n 23, at [80]; referred to in *Financial Markets Authority v CLSA Premium New Zealand Ltd* [2021] NZHC 2325, [2021] NZCCLR 16 at [30] and [94]; *Financial Markets Authority v Tiger Brokers (NZ) Ltd*, above n 5, at [33]–[34]; *Department of Internal Affairs v SkyCity Casino Management Ltd*, above n 21, at [23]–[24]; and *Department of Internal Affairs v Christchurch Casinos Ltd*, above n 21, at [40].

## Facts

*Overview*

[21] In November 2019, the Reserve Bank undertook an on-site inspection of ASB's compliance with the Act. This was a positive engagement with open and constructive conversations throughout the inspection. However, that inspection identified several issues relating to ASB's categorisation of customers as high risk and its ongoing customer due diligence on those customers. The Reserve Bank notified ASB of these issues in March 2020.

[22] In May 2023, the Reserve Bank undertook a further on-site inspection of ASB's compliance with the Act. ASB's constructive dialogue with Reserve Bank supervisors was again acknowledged. That inspection identified some of the same issues noted during the 2019 inspection. It also identified issues relating to ASB's resolution of transaction monitoring alerts and unusual activity reports, and ASB's prioritisation of alerts relating to terrorism financing and child exploitation. The Reserve Bank notified ASB of these issues on 13 December 2023, requiring remediation by 30 September 2024. That deadline was achieved, save that implementation of a new transaction monitoring system is ongoing.

[23] In addition to the Reserve Bank's oversight, ASB conducted and organised audits of various aspects of its compliance both prior to and during the relevant periods, including the following:

(a) in 2017, ASB's Audit and Assurance team audited ASB's AML/CFT programme;

(b) between October 2019 and February 2020, Ernst & Young (EY) conducted an independent validation of ASB's transaction monitoring daily reconciliation process; and

(c) between June and July 2022, ASB's Audit and Assurance team audited ASB's transaction monitoring function.

[24] Each of the above audits identified issues with ASB's AML/CFT transaction monitoring system and/or processes.

[25] In March 2024, the Reserve Bank commenced an investigation into ASB's compliance with the Act. ASB co-operated with the investigation, responding to three notices issued during 2024 and 2025 that requested various records, documents and information.

[26] Upon completion of the Reserve Bank's investigation, ASB immediately engaged with the Reserve Bank to resolve the proceeding. Within two months of the Reserve Bank's final notice, the parties had reached an agreed position on ASB's admission to seven civil liability acts and the quantum of an appropriate civil penalty.

*Predator as an AML/CFT monitoring and compliance tool*

[27] Prior to June 2013, ASB used an automated, centralised transaction monitoring system known as Predator for credit card fraud detection.

[28] In February 2012, Predator was independently assessed as suitable for broader use to meet ASB's monitoring requirements for AML/CFT over the next two to three years. As part of ASB's AML/CFT programme, Predator was loaded with rules to detect certain customer behaviours to determine whether enhanced customer due diligence or a suspicious activity report was required. However, it was recommended that ASB conduct a review of alert volumes and staffing requirements to reduce the risk that its monitoring team would be overwhelmed by alert volumes and subsequently fail to meet reporting requirements for suspicious activities.

[29] From July 2015, ASB was aware of limitations with Predator as a transaction monitoring system, including its capacity to hold alerts. From July 2017, ASB was aware of other issues (such as faulty prioritisations and alerts not being resolved within expected timeframes). In mid-2017, ASB's Audit and Assurance team identified that there were limitations with Predator because it was not specifically designed for the purpose of AML/CFT-related transaction monitoring. From August 2017, ASB's senior management was aware of Predator's issues and limitations.

[30] In October 2019, at ASB's request, EY started a review that identified several issues with ASB's manual reconciliation process through Predator. EY also noted the system was "unusual" from an AML/CFT perspective, because it made matching transactions with alerts unnecessarily complex. EY recommended that ASB consider building an instance of Predator dedicated solely to AML/CFT-related transaction monitoring and phase in a new AML/CFT transaction monitoring system.

[31] In May 2020, Predator's vendor informed ASB that Predator would not be supported from March 2021. ASB continued to use Predator after that time, supporting it internally.

[32] Between August 2020 and February 2021, ASB considered options for implementing a new transaction monitoring system and completed a request for proposals from prospective vendors. However, ASB prioritised other financial crime-related projects and put the transaction monitoring system upgrade on hold for 12 months.

[33] For a time, ASB attempted to build an instance of Predator dedicated solely to AML/CFT-related transaction monitoring, but this work was paused in July 2022. Around this time, ASB's Audit and Assurance team released its 2022 audit report about transaction monitoring. This noted that ASB's data flow architecture did not allow ASB to ensure that all of its activities were sufficiently covered by its transaction monitoring processes, no interim remediation measures had been put in place due to staff capacity issues and the prioritisation of other financial crime-related projects, and Predator's technical limitations limited ASB's ability to implement and manage the required transaction monitoring rules effectively and efficiently.

[34] Between December 2022 and March 2024, ASB selected and negotiated commercial terms with a vendor for a new transaction monitoring system to replace Predator. By 12 December 2025, this had still not been fully implemented.

*Transaction monitoring alerts and unusual activity reports*

[35] As described above, the Predator system used rules to detect certain customer behaviours to determine whether enhanced customer due diligence or a suspicious

activity report was required. If one of the preloaded rules was triggered, this generated alerts to be reviewed by analysts in ASB's Financial Crime Investigations (FCI) team. This involved an analyst considering the available information to determine whether the requisite suspicion existed for the purposes of making a suspicious activity report.

[36] ASB's Predator alerts were categorised as either standard or high priority.

(a) Prior to April 2021, alerts were classified as being high priority if the relevant transaction was undertaken by a high-risk customer based on ASB's risk rating model, a politically exposed person, or a person in respect of whom ASB had previously made a suspicious activity report, or if one of four rules related to potential terrorism financing was triggered.

(b) Between April 2021 and 1 June 2024, the risk rating methodology changed so high priority alerts were based on a customer's risk rating only. Otherwise, transactions related to potential terrorism financing and child exploitation were not characterised as being high priority.

(c) From 1 June 2024, alerts relating to terrorism financing and child exploitation were also characterised as high priority irrespective of the risk status of the customer.

[37] ASB's AML/CFT programme also provided for manual account monitoring, consisting of making unusual activity reports to escalate potentially suspicious activities for further analysis.

[38] The rules in the Predator system generated high volumes of alerts with high rates of false positives. Between September 2019 and February 2024, ASB experienced a backlog of processing both those alerts and unusual activity reports.

[39] Between 12 December 2019 and 28 February 2024, ASB failed to resolve the following within the relevant target timeframes:

(a) 121,366 Predator alerts involving transactions totalling approximately $12.1 billion (the longest period of time that an alert remained unresolved was 1,301 calendar days for a standard priority alert and 521 working days for a high priority alert); and

(b) 1,648 unusual activity reports involving transactions totalling approximately $66.2 million (the longest period of time that an alert remained unresolved was 654 calendar days for a standard priority alert and 638 calendar days for a high priority alert).

[40] Over time, ASB unsuccessfully attempted to address the backlog, including taking the following steps:

(a) Between 2019 and April 2022, it employed 20 additional full-time equivalent staff members.

(b) In April 2021, it introduced training to improve transaction reporting efficiency.

(c) In January 2022, it introduced a triage process for Predator alerts.

[41] In June 2022, ASB first began to make progress materially remediating the backlog. ASB engaged Deloitte to provide operational support to supplement the FCI team's capacity.

[42] On 20 February 2023, ASB disclosed the extent of the backlog to the Reserve Bank. ASB proposed to close certain alerts without review based on a methodology that had been developed by financial crime analytics and business assurance. On 29 August 2023, the Reserve Bank advised that it did not consider the proposal to be appropriate.

[43] From September 2023, ASB engaged Emagine Consulting UK to take over from Deloitte to provide operational support on the backlog issues. In addition, between August 2022 and January 2024, ASB employed 35 full-time equivalent staff members for the purpose of clearing the backlog, which was achieved on 8 February 2024.

Then, between March and April 2024, ASB employed a further 25 full-time equivalent staff members to ensure alerts were sustainably managed within ASB's target timeframes.

[44] The consequences of the failures to process alerts and unusual activity reports in a timely way were significant. Apart from the significant volume and value of transactions involved, ASB did not identify, or identify in a sufficiently timely manner, all customers in respect of whom enhanced customer due diligence should have been conducted or a suspicious activity report should have been made.

[45] During the relevant period, ASB filed 1,373 suspicious activity reports late, which involved transactions totalling approximately $60.71 million relating to its normal Predator operations (1,046 suspicious activity reports arose from Predator alerts concerning transactions totalling a value of $26.8 million, with the remaining suspicious activity reports having arisen from unusual activity reports involving transactions totalling a value of $33.91 million). In addition, ASB filed 63 late suspicious activity reports involving transactions totalling approximately $31.24 million for periods when ASB's Predator rules did not run correctly, so the rules were rerun later for the impacted time period after the problem was resolved (called backwash suspicious activity reports).

[46] ASB's processes required it to conduct enhanced customer due diligence on customers who engaged in the transactions that resulted in the late suspicious activity reports and backwash suspicious activity reports within a specified time of submitting a suspicious activity report in respect of those customers. ASB failed to do this for 1,061 of those customers engaged in transactions totalling approximately $70.9 million. Correspondingly, ASB was not permitted to continue its business relationships with those customers but failed to terminate these relationships.

*Foreign trust ongoing customer due diligence settings*

[47] Between September 2019 and February 2021, ASB's AML/CFT programme required ongoing customer due diligence to be conducted on high-risk customers every 18 months.

[48] From February 2021, ongoing customer due diligence on high-risk customers was required to occur whenever a specified mandatory trigger event took place and/or at set periodic frequencies. ASB considered its high-risk customers to include trusts domiciled outside of New Zealand and trusts with foreign beneficial owners (together foreign trusts).

[49] Between February 2021 and September 2024, absent a mandatory trigger event, ASB's AML/CFT programme only required ongoing customer due diligence to be conducted on a sample of foreign trusts, but no more than once in a three-year period. In practice, ASB selected and reviewed a monthly sample of foreign trusts from those not reviewed within the preceding three years. By contrast, absent a mandatory trigger event ASB was required to conduct ongoing customer due diligence on most other high-risk customers [redacted].

[50] The 2023 onsite inspection report identified that the sample approach for foreign trusts was inadequate, because it was possible that some foreign trusts presenting a high ML/TF risk would never have ongoing customer due diligence conducted on them. ASB responded by replacing the sampling approach to foreign trusts [redacted]. Until this correction was made, of the 3,666 foreign trust customers during the relevant period, ASB did not conduct ongoing customer due diligence on 2,624 (71.6 per cent). These customers engaged in 655,115 transactions totalling approximately $9.37 billion.

**Breaches**

[51] Reflecting the above facts, the breaches by ASB under the Act for which a penalty is sought are failures to:

(a) establish, implement or maintain an AML/CFT compliance programme that met the requirements in ss 56(1) and 57(1) of the Act insofar as they relate to:

(i) **First cause of action:** from at least 12 December 2019 until 30 September 2024, complying with customer due diligence requirements (s 57(1)(c));

(ii) **Second cause of action**: from at least April 2021 until 1 June 2024, setting out what ASB needed to do, or continue to do, to manage and mitigate the risks of money laundering and terrorist financing (s 57(1)(f)); and

(iii) **Third cause of action:** from at least 12 December 2019 until 12 December 2025, monitoring and managing compliance with ASB's procedures, policies and controls (s 57(1)(l));

(b) **Fourth cause of action:** conduct adequate ongoing customer due diligence on foreign trust customers during the period between 12 December 2019 and 28 February 2024 (s 31);

(c) **Fifth cause of action:** make suspicious activity reports to the Commissioner of Police within the timeframe required under the Act between 12 December 2019 and 28 February 2024 (s 40);

(d) **Sixth cause of action:** conduct enhanced customer due diligence on certain customers between 12 December 2019 and 28 February 2024 (s 22); and

(e) **Seventh cause of action:** terminate business relationships with the customers on whom it did not conduct compliant enhanced due diligence between 12 December 2019 and 28 February 2024 (s 37).

[52] It is not suggested that ASB was directly involved in money laundering, child exploitation or terrorism financing at any time.

[53] ASB nevertheless acknowledges that it failed to play its role in helping to detect financial crime and safeguarding New Zealand's financial system. ASB's failures were serious and took place over an extended period, and it accepts it did not act fast enough to resolve the problems. ASB has publicly apologised, admitted responsibility for its failures and undertaken remediation. It has improved its

AML/CFT systems and processes and has kept the Reserve Bank updated about these developments.

**Party submissions**

*Maximum amount*

[54] The maximum penalties prescribed by the Act for the civil liability acts committed by ASB are:

(a) for failing to establish, implement or maintain a sufficient AML/CFT compliance programme: $2 million each for the three breaches of this type;

(b) for failing to conduct customer due diligence (including both ongoing and enhanced customer due diligence): $2 million each for the two breaches of this type;

(c) for failing to report suspicious transactions: $2 million; and

(d) for failing to terminate existing business relationships: $1 million.

[55] Accordingly, the total maximum penalty available against ASB is $13 million for the seven causes of action.

*Starting point*

[56] The parties agree that the appropriate global starting point is $8.975 million, reflecting the totality of ASB's contraventions. This amounts to approximately 69 per cent of the available maximum penalty of $13 million.

[57] That overall starting point is based on aggregating the following sums for each cause of action:

(a) $1.85 million for failing to establish, implement or maintain an AML/CFT programme (relating to customer due diligence);

(b) $1.3 million for failing to establish, implement or maintain an AML/CFT programme (relating to managing and mitigating the risks of ML/TF);

(c) $1.85 million for failing to establish, implement or maintain an AML/CFT programme (relating to monitoring and managing compliance);

(d) $1 million for failing to adequately conduct ongoing customer due diligence;

(e) $1.1 million for failing to conduct compliant enhanced customer due diligence;

(f) $1.7 million for failing to report suspicious activities as required by s 40 of the Act; and

(g) $175,000 for failing to terminate existing business relationships.

[58] I address the details of the respective submissions of the parties on each cause of action in my analysis below.

*Aggravating and mitigating factors*

[59] The parties agree that there are no aggravating factors particular to ASB that require an uplift to the starting point.

[60] ASB has not previously been found to have contravened the Act, but it is accepted this is neutral, particularly when the non-compliance that is the subject of the proceeding spans a lengthy period of time.[26]

---

[26] *Department of Internal Affairs v Ping An Finance (Group) New Zealand Co Ltd*, above n 5, at [119]; *Department of Internal Affairs v Qian Duoduo Ltd*, above n 21, at [141]–[143]; *Department of Internal Affairs v OTT Trading Group Ltd,* above n 21, at [87]; and *Department of Internal Affairs v SkyCity Casino Management Ltd*, above n 21, at [97].

[61] The parties agree that ASB is entitled to a reduction of 25 per cent to reflect its co-operation and early admissions. ASB's co-operation and admissions enabled full resolution of the Reserve Bank's investigation at an early stage, before proceedings were issued.

*Totality*

[62] Questions of totality have been considered in arriving at the proposed penalty. The parties have sought to eliminate double-counting for conduct that constituted or led to different types of civil liability acts.[27]

[63] The Reserve Bank notes that a penalty of $6.731 million places ASB's conduct within the highest grouping of cases with a penalty in the range of 50−75 per cent of the maximum available (see [20] above). It submits that this appropriately reflects the seriousness and duration of ASB's contraventions, as well as the central position that banks occupy within the financial system.

**Analysis**

*Maximum amount*

[64] I accept the parties' submissions about the maximum penalties prescribed by the Act for each of the seven causes of action.

*First cause of action starting point*

[65] ASB accepts that it failed to establish, implement and maintain a fully compliant AML/CFT programme in respect of customer due diligence requirements. This encompasses two aspects: the resolution of automated and manual transaction monitoring alerts beyond the timeframes provided for in the programme; and the programme's inadequate settings for conducting ongoing customer due diligence on customers who were foreign trusts.

---

[27] Anti-Money Laundering and Countering Financing of Terrorism Act, s 74(2).

[66] As described above, due to Predator's limitations and the high number of false positives, ASB experienced a significant backlog of transaction monitoring alerts, the resolution of which exceeded ASB's internal timeframes. ASB's senior management was aware of the backlog from December 2019, but the steps taken to address it were patently inadequate. Meaningful progress was not made until June 2022, and the backlog was not cleared until 8 February 2024. This is an extensive period of non-compliance for a very significant volume and value of transactions. Meanwhile, as described in [47]–[50] above, between February 2021 and September 2024, ASB's programme settings for conducting enhanced due diligence in respect of foreign trusts were inadequate, even though foreign trusts were acknowledged as presenting a high ML/TF risk.

[67] The Reserve Bank notes that ASB's efforts to address these issues were under-resourced because of commercial prioritisation of other matters. It further submits that ASB's contravention is the worst of its kind to date in terms of the number and value of transactions involved.

[68] ASB's response to its use of the Predator system is addressed below under the third cause of action. ASB says resource and capability constraints impacted their decisions about project prioritisation. Meanwhile some interim solutions were implemented, but it is acknowledged those were inadequate.

[69] The closest comparators for the first cause of action are *Department of Internal Affairs v SkyCity Casino Management Ltd* (*SkyCity*) and *Department of Internal Affairs v Christchurch Casinos Ltd* (*CCL*).

(a) In *SkyCity*, a starting point of $1.5 million was used for an AML/CFT programme that was deficient in various respects, resulting in the late submission of 719 reports involving transactions with a value of over $1 billion, with the contraventions occurring over a period of 3.5 years, including failure to immediately remediate after the deficiencies were identified.[28]

[28] *Department of Internal Affairs v SkyCity Casino Management Ltd*, above n 21.

(b) In *CCL,* a starting point of $1.4 million was adopted for an AML/CFT programme that was deficient insofar as customer due diligence was concerned and contained practices that were contrary to the Act. These breaches occurred over a period of five years, including failure to remediate after the deficiencies were identified.[29]

[70] ASB accepts that the starting point in this case should be higher, given the following:

(a) ASB's contraventions persisted over a long time period (five years);

(b) the consequences associated with ASB's contraventions (including the value of the transactions involved);

(c) banks are high risk and play an important role in helping to detect financial crime and safeguarding New Zealand's financial system;

(d) ASB's size and position in that market; and

(e) the delay in remediation after the issues were identified was unacceptable, but counsel for ASB notes that this is also accounted for under the first two factors and was a feature present in both *SkyCity* and *CCL.*

[71] The jointly proposed starting point of $1.85 million (92.5 per cent of the maximum) is at the top end of the range to reflect these factors. I accept the suggested starting point for the first cause of action is appropriate in comparison with other cases, given these facts of systemic deficiencies not being properly remediated over a lengthy time despite awareness of them existing. The standards fell far below the expectations reasonably placed on registered banks to play their part in maintaining the integrity and reputation of New Zealand's financial system. Such conduct requires a strong deterrent response.

---

[29] *Department of Internal Affairs v Christchurch Casinos Ltd,* above n 21.

*Second cause of action starting point*

[72] As described in [36] above, between April 2021 and 1 June 2024, ASB's rules only triggered high priority alerts for transactions undertaken by high-risk customers. In all other cases, the alerts were classified as standard priority regardless of the inherent ML/TF risk of the underlying transactions. This failed to classify all transactions relating to terrorism financing and child exploitation as presenting a high ML/TF risk. The result was ASB's failure to identify, or identify in a timely way, all customers in respect of whom enhanced customer due diligence should have been conducted or a suspicious activity report made, in all circumstances where this should have occurred.

[73] This deficiency was first brought to ASB's attention by an internal audit report issued in September 2022, and then by the Reserve Bank in December 2023. It was not until 1 June 2024, however, that ASB changed its rules to prioritise alerts relating to terrorism financing and child exploitation.

[74] No previous case is entirely analogous. The parties place these facts between *CCL* (starting point of $1.2 million)[30] and *Reserve Bank of New Zealand v TSB Bank Ltd* (*TSB*) (starting points of $1.25 million and $1.375 million)[31] as different examples of AML/CFT programme contraventions, justifying a starting point of $1.3 million on the present facts:

(a) ASB's contravention was of a shorter duration but was larger in size and scale than CCL's failure to keep records for a five-year period;

(b) ASB's breach was systemic, but a very specific shortcoming (standard alerts were still triggered, and high priority was triggered for high-risk customers); and

(c) the delay in remediation after the issue was identified was unacceptable.

---

30 *Department of Internal Affairs v Christchurch Casinos Ltd,* above n 21.
31 *Reserve Bank of New Zealand v TSB Bank Ltd*, above n 22.

[75] For these reasons, I accept that a starting point of $1.3 million for the second cause of action is within range.

*Third cause of action starting point*

[76] The third cause of action is for using Predator for ASB's AML/CFT programme between 12 December 2019 and 12 December 2025, after ASB became aware of its limitations and that it was not fit for purpose in many respects. Further details are outlined in [27]–[34] above. Over a period of many years, these problems and the resulting backlog were not fully mitigated. Among other things, further resourcing was inadequate and ASB prioritised other financial crime-related projects.

[77] ASB says it could not progress all projects at the same time as it did not have the necessary specialist resource and capability to safely absorb the change represented by all projects. It submits that it made the risk-based decision to prioritise other financial crime projects and in the interim accept the risks associated with Predator (the need for an upgrade and the reconciliation issue identified by EY), subject to some interim solutions being implemented. Counsel for ASB emphasises that replacing the transaction monitoring system is a highly complex and sophisticated project that involves a total overhaul of ASB's existing systems.

[78] Both parties agree that *TSB* is the most useful comparator.[32] In that case a starting point of $1.25 million was adopted where TSB had no documented assurance measures in place between 2013 and 2016, despite the issue being brought to its attention in a 2015 audit report and a Reserve Bank inspection report in 2016, followed by a formal warning. TSB then implemented inadequate assurance measures for a further period of more than two years (the TSB board misunderstood whether the Reserve Bank regarded its measures as adequate).

---

[32] *Reserve Bank of New Zealand v TSB Bank Ltd*, above n 22.

[79] The parties agree that a higher starting point of $1.85 million is justified in this case:

(a) ASB is larger in size than TSB with greater financial means, as one of New Zealand's largest banks.

(b) The Reserve Bank regards the failure to remedy the breaches after notice as significantly more serious than *TSB*. While acknowledging that factor requires some weight, counsel for ASB emphasises that it compares favourably with *TSB* in some respects (ASB had some transaction monitoring systems in place throughout, it received no warnings from the Reserve Bank, and it acknowledged identified shortfalls and took steps to remediate them but was practically limited by technical capacity to implement all financial crime projects at once).

[80] Like the first cause of action, I accept that the jointly proposed starting point of $1.85 million (92.5 per cent of the maximum) is at the top end of the range to reflect the factual circumstances. The starting point for the third cause of action is appropriately higher than in *TSB*. These were systemic deficiencies not properly remediated over a lengthy time despite awareness of the problems. The standards fell far below the expectations reasonably placed on one of New Zealand's largest registered banks. Technical capacity constraints do not provide any excuse.

*Fourth cause of action starting point*

[81] As referred to in [47]–[50] above, during the relevant period, ASB failed to undertake adequate ongoing customer due diligence in respect of foreign trusts. This aspect is different from the first cause of action focused on the AML/CFT programme settings. This cause of action addresses the substantive failure to conduct ongoing customer due diligence on 2,624 foreign trusts during the relevant period.

[82] Other cases imposing penalties for breaches of s 31 of the Act are of limited utility, because they deal with account monitoring failures (with a maximum penalty of $1 million) rather than a failure to conduct ongoing customer due diligence.

[83] The parties suggest a starting point of $1 million (50 per cent of the maximum), taking into account the following:

(a) The conduct is less serious than the closest cases of account monitoring failures, which are *CCL* (involving a five-year breach that attracted a penalty of 85 per cent of the maximum penalty, being at the top end of the available range)[33] and *SkyCity* (involving 75 per cent of the maximum penalty being imposed for a five-year breach that was representative of the approach SkyCity took to account monitoring across its business).[34]

(b) This breach was for a period just over three years, in respect of approximately 0.1 per cent of ASB's business relationship customers in 2022 alone. Although the value of the transactions involved was up to approximately $9.37 billion, this is approximately 0.156 per cent of ASB's transactions in 2022 alone.

(c) The consequences of non-compliance are nevertheless significant, because of the high ML/TF risk posed by this type of customer.

(d) The starting point for this cause of action should be set at a level that avoids duplication with the penalty imposed in respect of the related first cause of action.

[84] I accept the submissions of both parties that the proposed starting point for the fourth cause of action is within range for the reasons they have given.

*Fifth cause of action starting point*

[85] The fifth cause of action is for the failure to report suspicious activity in accordance with the Act and outside of target timeframes. The extent of this contravention is summarised at [45] above.

---

33 *Department of Internal Affairs v Christchurch Casinos Ltd,* above n 21.
34 *Department of Internal Affairs v SkyCity Casino Management Ltd*, above n 21.

[86] The Reserve Bank refers to *Department of Internal Affairs v Ping An* (*Ping An*) (involving a starting point of $1.3 million for a failure to submit 173 suspicious activity reports)[35] and *Department of Internal Affairs v Jin Yuan* (*Jin Yuan*) (involving a starting point of $1.3 million for failing to report suspicious transactions and inadequacies with some of the 32 reports that were filed)[36] as instances where penalties were imposed for failures to submit suspicious activity reports. ASB submits those cases are of limited assistance because the conduct in those cases was more serious (total failures rather than late reports) but the consequences were more limited (lower numbers and value of transactions).

[87] However, counsel for ASB concedes that its contraventions under the fifth cause of action justify a higher starting point because ASB is one of New Zealand's largest banks, and the number of non-compliant suspicious activity reports is greater than in any previous penalty decision under the Act.

[88] For those reasons, I accept that the proposed starting point of $1.7 million (85 per cent of the maximum available) is within range.

*Sixth cause of action starting point*

[89] The sixth cause of action is for failure to conduct the enhanced customer due diligence within the expected timeframe on the customers who engaged in the transactions that resulted in late suspicious activity reports (both those arising from normal Predator operations and by backwash processes). The extent of this breach is described in [46] above.

[90] Three cases provide helpful comparisons:

(a) In *CCL*, a starting point of $900,000 was adopted in respect of a failure to conduct compliant enhanced due diligence in respect of 24 customers who undertook approximately $56.2 million in transactions that should

---

35 *Department of Internal Affairs v Ping An Finance (Group) New Zealand Company Ltd*, above n 5.
36 *Department of Internal Affairs v Jin Yuan Finance Ltd,* above n 21, at [23]–[24] and [40(d)].

have been subject to enhanced customer due diligence checks but were not.[37]

(b) In *Ping An,* a starting point of $1.3 million was adopted in respect of "contemptuous disregard" for AML/CFT requirements and a "widespread failure" to conduct compliant customer due diligence in respect of 1569 transactions, including a failure to conduct due diligence in respect of 362 customers.[38]

(c) In *SkyCity*, a starting point of $1.6 million was adopted in respect of a failure to conduct enhanced due diligence on 116 customers involving transactions totalling just over $1.065 billion. SkyCity had been warned in 2014, 2019 and 2020 that some of its enhanced due diligence practices were non-compliant.[39]

[91] The parties suggest a starting point of $1.1 million (55 per cent of the maximum), taking into account the following:

(a) ASB's contravention is most comparable to, though more serious than, than in *CCL*.

(b) ASB's status as a bank, as well as its size and position in the banking sector, elevates the seriousness of its conduct.

(c) A starting point substantially lower than that in *SkyCity* is warranted given the significantly lower transaction value and the absence of any prior warnings from the Reserve Bank.

[92] For those reasons, I accept that the proposed starting point of $1.1 million (55 per cent of the maximum available) is within range.

---

37 *Department of Internal Affairs v Christchurch Casinos Ltd,* above n 21.
38 *Department of Internal Affairs v Ping An Finance (Group) New Zealand Co Ltd,* above n 5, at [6], [41] and [105].
39 *Department of Internal Affairs v SkyCity Casino Management Ltd*, above n 21.

*Seventh cause of action starting point*

[93] The seventh cause of action is the related failure to terminate existing business relationships where adequate customer due diligence had not been completed. Care needs to be taken to avoid double counting where this arises from the same conduct addressed in the sixth cause of action.[40]

[94] In *CLSA*, Edwards J considered the nature of the obligations to be different,[41] and adopted a discrete starting point of $50,000 for the reporting entity's failure to terminate business relationships when required, reduced from the $150,000 starting point that would otherwise have been appropriate had the termination failure been considered on a standalone basis. That approach of applying the totality principle has been followed in subsequent cases.[42]

[95] Adopting that approach, the parties submit a starting point of $175,000 (17.5 per cent of the maximum) is appropriate for the seventh cause of action:

(a) In *CCL*, the Court adopted a starting point of $150,000 in respect of CCL's failure to terminate business relationships with 24 customers, in circumstances where the Court considered a starting point of $400,000 to $500,000 would have been appropriate on a standalone basis.

(b) In *SkyCity*, the Court adopted a starting point of $200,000 in respect of SkyCity's failure to terminate business relationships which enabled over $1.065 billion to be transacted through SkyCity, noting that a starting point of between $550,000 to $700,000 would have been warranted on a standalone basis.

(c) It is submitted that ASB's failures to terminate business relationships fall between the above two examples. On a standalone basis, the Reserve Bank suggests that a starting point of between $500,000 and

---

40 Anti-Money Laundering and Countering Financing of Terrorism Act 2009, s 74.

41 *Financial Markets Authority v CLSA Premium New Zealand Ltd,* above n 5, at [57].

42 *Financial Markets Authority v Tiger Brokers (NZ) Ltd,* above n 5, at [48]; *Department of Internal Affairs v SkyCity Casino Management Ltd*, above n 21, at [93]; and *Department of Internal Affairs v Christchurch Casinos Ltd,* above n 21, at [65]–[66].

> $600,000 would have been warranted for a breach involving 1,061 customers and transactions totalling approximately $70.9 million.

[96] I accept that the proposed starting point of $175,000 is appropriate for the seventh cause of action (17.5 per cent of the maximum).

*Aggravating and mitigating factors*

[97] There are no aggravating features personal to ASB that require an increase to the individual starting points or overall total.

[98] ASB is entitled to a reduction for its co-operation and early admissions. This enabled full resolution of the Reserve Bank's investigation at an early stage, before proceedings were issued. Consistent with other cases where such a positive and pro-active approach was adopted at an early stage, I accept that a reduction of 25 per cent is warranted in this case.[43]

[99] I acknowledge that ASB has fully remediated some breaches and is continuing to remediate the balance. However, this reflects the Act's requirements and is not a ground for any further reduction.[44]

*Totality*

[100] As addressed above, the parties' suggested starting points account for any overlap in ASB's breaches to ensure there is no double-counting in the overall penalty reached.

[101] While I have considered the appropriateness of the starting point for each cause of action, it is the overall penalty that is most important, rather than how it is calculated. Standing back and looking at the matter overall, I find that the proposed

---

43 *Reserve Bank of New Zealand v TSB Bank Ltd*, above n 22, at [53]–[56]; *Financial Markets Authority v Tiger Brokers (NZ) Ltd,* above n 5, at [63]; and *Department of Internal Affairs v SkyCity Casino Management Ltd*, above n 21, at [101].

44 *Department of Internal Affairs v Qian Duoduo Ltd,* above n 21, at [162], *Financial Markets Authority v CLSA Premium New Zealand Ltd,* above n 5, at [90]; *Financial Markets Authority v Tiger Brokers (NZ) Ltd,* above n 5, at [64]; and *Department of Internal Affairs v SkyCity Casino Management Ltd*, above n 21, at [98].

pecuniary penalty of $6.731 million reflects the particular circumstances of this case and satisfies the objectives of the Act. ASB's failures were serious and took place over an extended period. Its conduct fell far below the expectations reasonably placed on registered banks to play their part in maintaining the integrity and reputation of New Zealand's financial system. Such conduct requires a strong response to provide general deterrence, and to encourage cooperation and corrective action when contraventions of the Act are identified.

[102] I am satisfied that the proposed overall penalty of $6.731 million achieves those objectives and is within the appropriate range for these seven causes of action.

**Non-publication orders**

[103] The courts have an inherent power to make orders to protect confidential information in civil proceedings, including to protect trade secrets or commercially sensitive information.[45]

[104] Personal, private and confidential information can be the subject of non-publication orders in pecuniary penalty proceedings under the Act:[46]

> Section 46 of the Anti-Money Laundering and Countering Finance of Terrorism Act 2009 contains restrictions on the disclosure of information relating to suspicious activity/transaction reports which is said to be relevant to some of the matters addressed in the agreed statement of facts and notice of admission.
>
> I accept that this type of information would need to be redacted before access was granted. Redacting this information would protect the confidentiality and privacy interests of those parties, and ensure that only information that is necessary to satisfy the principle of open justice is disclosed.

[105] At the hearing, I accepted ASB's submissions that the statement of claim contains details of ASB's existing financial crime detection and investigation settings which, if made public, could be exploited by third parties in ways that would undermine their effectiveness. Also, disclosure of some employee information was unnecessary to understand the subject matter of the proceeding. I requested the parties to confer on a redacted version of the statement of claim that excludes the sensitive

---

45 *Erceg v Erceg* [2016] NZSC 135; [2017] 1 NZLR 310 at [5]–[7] and [13].
46 *Financial Markets Authority v CLSA Premium New Zealand Ltd* [2021] NZHC 933 at [22]–[23].

and private information of this nature. I now record the corresponding non-publication orders below.

[106] Counsel are invited to file memoranda within five working days if any aspects of this judgment require redaction for the same reasons.

**Result**

[107] I enter judgment for the Reserve Bank on the seven causes of action pleaded in its statement of claim.

[108] I order ASB to pay an overall pecuniary penalty of $6,731,000.

[109] I make an order prohibiting the publication of the following material from the statement of claim and any related reference to that content in the parties' submissions:

(a) internal time periods or targets in ASB's AML/CFT compliance programme, and ASB's current approach to reviewing foreign trusts; and

(b) any reference to the identities of specific ASB employees (or former employees) who are not parties to the proceeding.

[110] A redacted statement of claim complying with the above publication restrictions has been filed along with a memorandum of counsel for ASB dated 5 March 2026.

_____

O'Gorman J