IN THE HIGH COURT OF NEW ZEALAND
WELLINGTON REGISTRY

I TE KŌTI MATUA O AOTEAROA
TE WHANGANUI-A-TARA ROHE

CIV 2021-485-296
[2021] NZHC 2241

UNDER	the Anti-Money Laundering and Countering Financing of Terrorism Act 2009
BETWEEN	RESERVE BANK OF NEW ZEALAND Plaintiff
AND	TSB BANK LIMITED Defendant

Hearing:	22 July 2021
Counsel:	R S May and V M Rea for Plaintiff E J Rushbrook and E M Light for Defendant
Judgment:	27 August 2021

JUDGMENT OF MALLON J

Table of contents

Introduction

[1] This proceeding concerns acknowledged breaches of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (the Act) by TSB Bank Limited (TSB). The breaches concern internal procedures that the Act requires a financial institution to have. These internal procedures are intended to support the more substantive obligations under the Act to collect and verify information and to report suspicious transactions.

[2] Breaches of these requirements give rise to civil liability for which the Court can impose a pecuniary penalty. The Reserve Bank of New Zealand (RBNZ), the supervisor of TSB's compliance with these requirements, and TSB have agreed on what they regard to be an appropriate penalty.[1] The total proposed penalty is $3.85 million. They seek that the Court impose this penalty. The Court's role in such circumstances 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]

---

1 In relation to TSB's real estate work, the Department of Internal Affairs would typically be the supervisor but, pursuant to a notice under s 130(2) of the Act, RBNZ is the supervisor for this work as well as TSB's banking business.

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

Background

The Act

[3] The Act came into force on 30 June 2013. Its purpose is to detect and deter money laundering and the financing of terrorism, to maintain and enhance New Zealand's international reputation, and to contribute to public confidence in the financial system.[3] It imposes requirements on certain kinds of businesses (referred to as reporting entities), broadly those that are in the business of managing financial transactions on behalf of clients. It includes financial institutions and real estate businesses.[4]

[4] Under Part 2 of the Act, reporting entities are required to:

(a) conduct customer due diligence (CDD);

(b) report suspicious activity;

(c) keep proper records of transactions, customers and suspicious activity reports;

(d) conduct and review a risk assessment for all regulated aspects of their business; and

(e) maintain adequate and effective systems for a complete and regularly reviewed compliance programme (referred to as an AML/CFT programme).[5]

[5] This proceeding concerns the risk assessment and AML/CFT programme requirements. These requirements are intended to ensure that reporting entities can fulfil their CDD and reporting obligations.

---

3 Section 3.
4 Section 5.
5 AML/CFT means anti-money laundering and countering the financing of terrorism. An AML/CFT programme is defined in s 5 as a compliance programme established under s 56(1) of the Act.

[6] The risk assessment and AML/CFT programme requirements are set out in subpart 4 of Part 2.[6] These provisions include:

(a) A requirement to establish, implement and maintain an AML/CFT programme that includes internal procedures, policies, and controls to detect, and manage the risk of, money laundering and the financing of terrorism (s 56).

(b) The minimum requirements for an AML/CFT programme (s 57). These are that:

(i) the AML/CFT programme be in writing;

(ii) it be based on a risk assessment undertaken in accordance with s 58; and

(iii) it includes adequate and effective procedures, policies, and controls for specific matters, including "monitoring and managing compliance with, and the internal communication of and training in, those procedures, policies and controls" (s 57(1)(l)).[7]

(c) The requirements for a risk assessment (s 58). These are that:

---

6 Subpart 1 concerns CDD requirements, subpart 2 concerns suspicious activity reports, subpart 3 concerns record keeping and subpart 4 concerns risk assessment and AML/CFT programme requirements.

7 The other matters are: vetting relevant employees (s 57(1)(a)); training relevant employees (s 57(1)(b)); complying with CDD requirements (s 57(1)(c)); reporting suspicious activities and prescribed transactions (s 57(1)(d) and (da)); record keeping (s 57(1)(e)); steps to manage and mitigate risks (s 57(1)(f)); examining and keeping written findings of unusual transactions or activities (s 57(1)(g)); monitoring and keeping written findings relating to business relationships and transactions involving countries with inadequate AML/CMT systems and having additional measures for dealings with such countries (s 57(1)(h)); preventing the use of products and transactions that might favour anonymity (s 57(1)(i)); determining when particular kinds of CDD are appropriate (s 57(1)(j)); and providing for when and how others may conduct the CDD on behalf of the reporting entity (57(1)(k)).

(i) the reporting entity undertakes an assessment of the risk of money laundering and financing of terrorism that it may reasonably expect to face in the course of its business;

(ii) in assessing the risk, it has regard to certain matters which include "the countries it deals with" (s 58(2)(e)); and

(iii) its risk assessment be in writing and cover the identified risks and how it will ensure its assessment remains current, and enable the entity to determine its level of risk.

(d) A requirement to review the risk assessment and AML/CFT programme to ensure it is up to date, to identify deficiencies in its effectiveness and to make any necessary changes (s 59(1)).

(e) Regular audit requirements (ss 59(2), 59A and 59B).

[7] The Act provides for AML/CFT supervisors. Their functions include monitoring, investigating and enforcing reporting entities' compliance with the Act's requirements.[8] Their powers include conducting on-site inspections.[9] Where the relevant AML/CFT supervisor of a reporting entity considers that the entity has failed to comply with any of the AML/CFT requirements, it may take a range of actions including issuing a formal warning or applying to the High Court for the imposition of a pecuniary penalty.[10] A failure to comply with any of the AML/CFT requirements is termed a "civil liability act".[11]

[8] The maximum pecuniary penalty depends on the nature of the breach. Some breaches have a maximum penalty of $100,000 for an individual and $1 million for a body corporate. Others, including failing "to establish, implement or maintain an AML/CFT programme", have a maximum of $200,000 for an individual and $2 million for a body corporate.[12]

---

8 Section 131.
9 Section 132.
10 Section 79.
11 Section 78.
12 Section 90.

[9] In determining the appropriate penalty, the Court must have regard to all relevant matters. This includes:[13]

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

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

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

(d) whether the person has been found by the court to have engaged in any similar conduct previously.

TSB

[10] TSB is a small and proudly New Zealand-owned bank headquartered in Taranaki. It has an ownership structure under which its profits go to its philanthropic shareholder (at the relevant time the TSB Community Trust, and now known as the Toi Foundation).[14]

[11] TSB provides retail banking in New Zealand. It does not have an overseas operation. It is New Zealand's seventh largest registered bank in terms of total assets, holding approximately 1.35 per cent of industry assets, two per cent of customer deposits, and a two-three per cent share of branches during the relevant period. Its annual revenue ranged from $124.6 million to $164.5 million and its profit before tax ranged from $33.5 million to $88.5 million during the relevant period.

[12] TSB also operated a realty business. This operation was based in New Plymouth and served the surrounding areas. It was a small operation relative to its banking business as measured by revenue, profit and number of those working for it. TSB sold its realty business on 22 October 2020.

---

13 Section 90(4).

14 TSB is owned by Toi Foundation Holdings Limited (formerly TSB Group Limited), a wholly owned subsidiary of Toi Foundation (formerly TSB Community Trust), which is an independent body.

[13] TSB has been a reporting entity in respect of its banking operations since 30 June 2013 (when the Act came into force). It was also a reporting entity in respect of its realty operations during the period from 1 January 2019 (from when the Act first applied to real estate businesses) until 22 October 2020.

[14] TSB's admitted breaches are in four categories:

(a) first, its AML/CFT programme did not have adequate and effective procedures, policies and controls for "monitoring and managing compliance with, and the internal communication of and training in, those procedures, policies, and controls" (the parties have referred to this as documented assurance measures) as required by s 57(1);

(b) second, TSB failed to review and maintain its AML/CFT programme as required by ss 56 and 59;

(c) third, TSB failed to conduct an adequate risk assessment in respect of its realty operations as required by s 58; and

(d) fourth, TSB failed to have regard to certain countries it deals with in conducting its risk assessment as required by s 58(2)(e).

[15] There is no suggestion that there has been any financing of terrorism or money laundering in relation to financial transactions through TSB. Nor is there any suggestion that TSB was intentionally failing to comply. Rather, aspects of its risk assessment and AML/CFT programme were inadequate and were not reviewed when they should have been.

[16] TSB is disappointed to have found itself before the Court. It takes the admitted breaches seriously. It has fully cooperated with RBNZ in its investigation and this proceeding and in resolving the matter appropriately. It has undertaken a full remediation exercise and RBNZ has indicated it is satisfied with the progress TSB has made.

Audits

[17] An independent audit of a reporting entity's risk assessment and AML/CFT programme is required every two years.[15] In accordance with this, independent audits were undertaken in:

(a) 2015: for the period 31 June 2013 to 31 May 2015 (AML report dated 22 July 2015);

(b) 2017: for the period 1 April 2016 to 31 March 2017 (Deloitte report dated 20 June 2017 and management letter dated 24 July 2017); and

(c) 2019: for the period 1 April 2017 to 31 March 2019 (Deloitte report dated 19 August 2019 and management letter dated 25 July 2019).

On-site inspections

[18] Pursuant to its power to conduct site inspections, RBNZ conducted on-site inspections on 29-31 October 2013, 9 June 2016, 10-11 October 2017 and 30-31 July 2019. RBNZ provided a report to TSB for each of these inspections.

[19] RBNZ issued a formal warning to TSB on 28 November 2016 following the 2016 on-site inspection. RBNZ's view was that TSB had not reviewed and kept up to date its risk assessment between 30 June 2013 and 9 June 2016. TSB was told that it must "immediately review its risk assessment, and amend any deficiencies" in order to fulfil the minimum requirements of the Act. It was also told that it must ensure "ongoing adherence to its procedures, policies and controls" in relation to these requirements. It was warned that ongoing failures could lead to penalties under the Act.

---

[15] Section 59(2).

First breach

Summary

[20] Documented assurance measures are one of the minimum requirements of an AML/CFT programme (s 57(1)(l)). The purpose of these measures is to ensure that a reporting entity's procedures, policies and controls for the other requirements of an AML/CFT programme (s 57(1)(a)-(k)) are working effectively. RBNZ alleges and TSB accepts that between 2013 and 2019, TSB's AML/CFT programme did not contain adequate and effective documented assurance measures.

[21] The parties agree that a penalty of $1,062,500 is appropriate for TSB's breach of these obligations. They have arrived at this penalty by taking a starting point of $1.25 million, applying an uplift of five per cent because the breach occurred after RBNZ issued a warning to TSB in 2016, and then applying a 20 per cent discount to reflect TSB's admission of liability and cooperation.

Circumstances

[22] At the outset TSB had no documented assurance measures in place. This was still the case at the time of the 2015 audit. The 2015 audit report identified this. It said that, although TSB's Compliance Officer was active in key areas of assurance, its AML/CFT assurance framework was not yet "formalised over the wider obligations of the Act". It recommended that work towards finalising that framework continue "as a matter of priority", with regular testing of key operational areas and regular reporting to management and the board.

[23] Documented assurance measures were also not in place at the time of RBNZ's October 2016 on-site inspection. Following this inspection, RBNZ issued a written warning (on 28 November 2016). This was focussed on TSB's risk assessment not having been reviewed and kept up to date. However, it also stated that TSB had not complied with the obligation under s 59(1) to "identify any deficiencies in the effectiveness of … the AML/CFT programme" and to make any changes identified as necessary.

[24] As part of its response to the inspection (and subsequent written warning), from 27 October 2016 TSB had in place a document titled "Operational Assurance Programme". This was a documented assurance measure. It was, however, inadequate because:

(a) it was directed only to TSB's procedures, policies and controls for complying with CDD requirements for new customers (referred to as onboarding) and did not address the assurance measures for the other components of its AML/CFT programme;[16]

(b) in relation to onboarding, it did not address measures for monitoring and managing the internal communication of and training in onboarding procedures, policies or controls, and nor for ongoing CDD and account monitoring;[17] and

(c) it did not have measures to identify whether the onboarding controls it had put in place were appropriately implemented and were operating effectively.

[25] TSB had also commissioned a broad Risk Management and Compliance Report from Deloitte. In December 2016 TSB put in place an action plan intended to implement the recommendations of Deloitte. Amongst other things, it was intended to supplement the operational assurance programme in order to meet the requirements of s 57(1)(l).

[26] However, material progress in relation to the operational assurance programme had not been made by the time of the 2017 audit. The 2017 audit report found that the monitoring activities that were part of the operational assurance programme were not undertaken by a fully independent TSB team and the monitoring activities were limited in scope.

---

16 Section 57(1)(a)-(b) and (d)-(k).
17 Section 57(1)(c).

[27] In response to this finding, management commented that remediation action (to develop and implement a comprehensive AML/CFT monitoring and compliance programme) was to be completed by the end of September 2017. TSB Board committees received updates of progress. However, in September 2017 the remediation action was still not completed.

[28] At RBNZ's on-site inspection in October 2017 the remediation topics covered risk assessment, termination of customer relationships, transaction monitoring, and accuracy of annual report data. It did not cover TSB's compliance with s 57(1)(l). Following this inspection, RBNZ provided a report dated 23 November 2017. This report recorded that, during the on-site visit, RBNZ obtained an assurance that TSB had taken the steps to address the breach referred to in the formal warning and "has adequate and effective procedures, policies, and controls in place to ensure ongoing compliance with sections 57(1), 58 and 59(1)" of the Act.

[29] Between the end of 2017 and the beginning of 2018, remediation progress was disrupted by personnel changes within TSB, with the Chief Executive Officer, Deputy Chief Executive Officer, Chief Risk Officer and Head of Compliance all ceasing to work for TSB. A new Head of Operational Risk and Compliance joined TSB in March 2018. This appointee received no handover or guidance because the Chief Risk Officer and Head of Compliance had already left.

[30] In May 2018 work was again underway. This included TSB conducting a targeted onboarding review of 52 trust customer files in that month. This found that only 23 per cent of files showed compliance with all CDD requirements, 52 per cent of files showed compliance with some CDD requirements, and 25 per cent of files showed compliance with few or no CDD requirements.

[31] A misunderstanding then arose about whether TSB was in full compliance. TSB's internal audit partner reported to the Board's audit committee on 16 May 2018 that RBNZ was satisfied that it had adequate, policies and controls in place. TSB accepts that it misinterpreted RBNZ's report of 23 November 2017 in forming that view. RBNZ accepts there was no bad faith by TSB in this.

[32] However, this misunderstanding meant that relevant information had not been considered when the Board approved the new Compliance Roadmap, which the Head of Operational Risk and Compliance presented in July 2018. TSB continued its work on the new Compliance Roadmap but it was not prioritised because of the misunderstanding that the RBNZ considered TSB to be compliant.

[33] Further internal reviews of the effectiveness of onboarding controls took place:

(a) In April 2019 TSB's internal audit partner undertook a "deep dive" into onboarding accuracy as a follow up from the May 2018 targeted review. This found that between 83 per cent and 87 per cent of customer files sampled complied with CDD requirements.[18] It also found that monthly sample testing used for checking compliance with the Act was inefficient and did not provide representative or useful results.

(b) An internal audit of one of TSB's branches on 23 July 2019 identified ongoing deficiencies and that target sample reviews by the branch manager had not been completed.

(c) TSB's compliance report for the end of July 2019, which was based on quality assurance samples from each branch, showed significant numbers of onboarding errors in the sample checks, with overall accuracy of 86 per cent and three branches with accuracy of between 70 per cent and 80 per cent for April to July 2019.

[34] External reviews also showed that the controls for onboarding were not operating effectively:

(a) Sampling undertaken by RBNZ during its July 2019 on-site inspection identified that seven out of 20 customer files reviewed showed onboard failures. Four of these files had been updated with the required

[18] This appears to have been a significant improvement from the May 2018 targeted review but still illustrated compliance gaps.

information between the time that RBNZ had provided TSB with a list of customer files for sampling and the on-site inspection.

(b) The 2019 Deloitte report identified from sample testing a significant level of non-compliance with TSB's CDD policy and a risk that TSB was not performing the correct level of CDD for certain customer types.[19]

[35] The 2019 Deloitte report also found that TSB had some limited monitoring activities in place as part of their operational assurance programme. However, these activities were not undertaken by a fully independent TSB team and the activities were limited and did not address all aspects of TSB's work programme.

[36] Throughout all of this, the Board received regular updates from TSB management in relation to the AML/CFT programme. From February 2018 senior management and the Board mistakenly believed that RBNZ considered its AML/CFT programme to be compliant. While the 2019 Deloitte audit report re-identified the absence of documented assurance measures, that report was received one week after RBNZ's 2019 on-site inspection.

[37] All of this meant that TSB did not have adequate documented assurance measures for six years. The 2017 Deloitte report identified that TSB had not designed an appropriate monitoring programme to identify whether controls were appropriately implemented and operating effectively as designed. Both TSB and external reviews showed that the controls they did have were not operating effectively as designed. The misunderstanding that arose in 2018 meant that priority was not given to this work. As a result, by the time of the 2019 on-site inspection, no further documented assurance measures had been established.

---

[19] Under this breach, RBNZ does not allege failures by TSB to comply with CDD or prescribed and suspicious transaction reporting requirements. The allegation relates only to having inadequate documented assurance measures (necessary to provide assurance of compliance with the other requirements).

Remediation and cooperation

[38] On receipt of the 2019 Deloitte report, TSB's Board and senior management took immediate steps to improve TSB's compliance with the Act. This included developing documented assurance measures. RBNZ's desktop review indicates that these are likely to be sufficient.

[39] TSB cooperated fully with RBNZ from the outset. This included full cooperation during the investigation (including providing extensive discovery) and in the proceedings before the Court, which has resulted in the agreed position presented to the Court.

Penalty

[40] The parties have agreed upon the proposed starting point based on a scale of culpability levels (low, medium, high, very high) as against the maximum penalty.[20] As this breach relates to having an inadequate AML/CFT programme, they are agreed that it comes within the $2 million maximum (which applies to a reporting entity who fails to establish, implement or maintain an AML/CFT programme).

[41] They are agreed that this first breach falls within the middle of their proposed "high culpability" band and that the starting point should therefore be set in the middle of 50 to 75 per cent of the maximum. They have therefore proposed a starting point of $1.25 million. In agreeing to a middle of high culpability they consider there to be two key aggravating factors. The first is the lengthy time over which TSB had an inadequate AML/CTF programme. The second is that, as a registered bank (albeit not one of the largest banks), TSB is much larger and has more central role in New Zealand's financial systems relative to other classes of reporting entities. Systemic failures of the kind here therefore create a risk to confidence in New Zealand's financial systems generally.

---

[20] This methodology has low culpability at up to 25 per cent of the maximum; medium at 25 to 50 per cent of the maximum; high culpability at 50 to 75 per cent of the maximum; and very high culpability at 75 to 100 per cent of the maximum.

[42] I agree with the parties that the main culpability factors are the length of time over which the failure occurred and the size and status of TSB as a registered bank. There are several factors that reduce its seriousness. This was not a case of TSB failing to implement any AML/CFT programme. Rather, the breach related to one component (albeit an important component) of that programme. It was not a deliberate failure and some steps were taken to implement assurance measures. The failure continued as long as it did in part because of a misunderstanding that its measures were now regarded as adequate and it was not helped by a significant change in senior personnel and the absence of a handover.

[43] I consider that, especially when there have limited cases against which to compare relative seriousness of breaches, forming a view on their seriousness with reference to general bands from low to high (or very high) is a logical and appropriate way of assessing where the starting point should be. Overall, I might have put culpability at around the upper end of medium (using the parties' categories) reflecting the factors that reduce the culpability and that TSB, while a large financial institution, is not of the size of the largest banks operating in New Zealand. However, this is not an exact science, and I am prepared to accept that the parties are not out of range in assessing it at a little over 60 per cent of the maximum especially in view of the period over which the breach extended. I therefore accept the starting point is within range although it is arguably towards the high side of the range.

[44] The parties agree that the starting point should be uplifted by five per cent. Although the formal warning in 2016 concerned TSB's failure to review its risk assessment, the parties agree that it ought to have led to TSB ensuring its AML/CFT programme was current and fulfilled the minimum requirements of the Act. Further, the 2017 Deloitte report also put TSB on notice that it did not have appropriate monitoring programmes to identify whether its controls were being appropriately implemented and operating effectively. I have no issue with this uplift (the reasons why the parties have agreed to it support it), nor with the parties' agreement that no uplift is appropriate for senior knowledge or complicity (given the misunderstanding that arose about whether RBNZ was satisfied that TSB's programme was compliant).

[45] The parties agree that TSB's admission and cooperation entitles it to a substantial reduction. They have agreed to a discount of 20 per cent to reflect this. In support of this, they refer to *Department of Internal Affairs v Qian DuoDuo Ltd* where a 20 per cent discount was allowed for the defendant's admission of liability, cooperation and subsequent steps to ensure compliance.[21]

[46] However, the cooperation in that case appears not to have been to the same extent as that here. The Judge in *Qian DuoDuo* noted, for example, that "although generally cooperative with the DIA investigation", the defendant had inaccurately represented the nature of its relationship with six money remitters.[22] And although the defendant had admitted liability following negotiations, and had also agreed a detailed and comprehensive statement of agreed facts and widespread breaches of the Act, they had not agreed on the penalty.[23]

[47] Therefore, based on a comparison with *Qian DuoDuo*, a discount of 20 per cent here seems light. This was the only case the parties relied on to support the discount they have proposed. However, the discount is also light in comparison with *Department of Internal Affairs v Jin Yuan Finance Limited*, the other proceeding for pecuniary penalties under the Act in which a discount was allowed.[24] In that case, the Judge allowed a 15 per cent discount. This was because the defendant admitted the breaches but had not admitted the particulars of them (and nor was there agreement to the appropriate penalties). The Judge did not allow a discount for cooperation because the defendant provided vague or misleading information to the DIA and had failed to rectify its non-compliance.[25]

[48] It is also light in comparison with the discounts allowed in comparable complex regulatory proceedings for pecuniary penalties. For example, in *Commerce*

---

21 *Department of Internal Affairs v Qian DuoDuo Ltd* [2018] NZHC 1887 at [163].

22 At [4].

23 At [6].

24 *Department of Internal Affairs v Jin Yuan Finance Limited* [2019] NZHC 2510 at [43] and [44].

25 The two other cases under the Act involved no discounts. In *Department of Internal Affairs v OTT Trading Group Limited* [2020] NZHC 1663, the defendants had failed to cooperate, were not candid in the investigation and intentionally misled the DIA. They also did not admit liability with the hearing proceeding by formal proof. In *Department of Internal Affairs v Ping An Finance (Group) New Zealand Company Ltd* [2017] NZHC 2363, the defendant had not accepted responsibility and did not cooperate in rectifying the breaches.

Commission v Aurora Energy Ltd the electricity lines company admitted to failing to achieve Quality Standards under the Commerce Act 1986.[26] As part of the agreed penalty submitted to the Court for approval, the parties had agreed to a discount of 38 per cent for full cooperation. This discount was approved by the Court as within range. There was full cooperation with the investigation, early acceptance of liability and significant work towards future compliance. That discount was in line with the 35 per cent discount in *Commerce Commission v Vector Ltd* under the same regulatory regime.[27]

[49] For pecuniary penalties for anti-competitive conduct in breach of the Commerce Act, discounts have been in the range of 25 per cent for early admission of responsibility but no active cooperation,[28] between 25 per cent and 30 per cent for early admission and full cooperation,[29] and more where there has been additional assistance by giving evidence in proceedings against others.[30]

[50] A discount of 30 per cent was allowed for admitted breaches under the Financial Markets Conduct Act 2013 and full cooperation.[31] Discounts of 35 per cent have been allowed in Fair Trading Act prosecutions for early guilty pleas and cooperation.[32]

[51] In the criminal jurisdiction, an early guilty plea typically attracts a 25 per cent discount with an additional discount available if there is demonstrated remorse. In *Hessell v R*, the Supreme Court explained that guilty pleas delivered benefits to the administration of justice and to those who must otherwise participate in the trial

---

26 *Commerce Commission v Aurora Energy Ltd* [2020] NZHC 610.

27 *Commerce Commission v Vector Ltd* [2019] NZHC 540.

28 *Commerce Commission v PGG Wrightson Ltd* [2015] NZHC 3360; *Commerce Commission v Rural Livestock Ltd* [2015] NZHC 3361; and *Commerce Commission v Unique Realty Ltd* [2016] NZHC 1064.

29 *Commerce Commission v First Gas Ltd* [2019] NZHC 231; *Commerce Commission v GEA Milfos International Ltd* [2019] NZHC 1426; and *Commerce Commission v Property Brokers Ltd* [2017] NZHC 681.

30 *Commerce Commission v Lodge Real Estate Ltd* [2016] NZHC 3115; and *Commerce Commission v Lodge Real Estate* [2017] NZHC 1875.

31 *Financial Markets Authority v ANZ Bank New Zealand Ltd*, above n 2.

32 *Commerce Commission v Steel & Tube Holdings Ltd* [2020] NZCA 549; *Commerce Commission v Callplus Services Ltd* [2020] NZHC 2655; *Commerce Commission v Brilliance International Ltd* [2018] NZDC 7359; *Commerce Commission v Timber King Ltd* [2018] NZDC 510; and *Commerce Commission v Topline International Ltd* [2017] NZDC 9221.

process.[33] The courts have recognised that admission of liability and cooperation in regulatory cases are also in the public interest and the discount allowed should reflect this.

[52] In Commerce Act cases for example, where there are often significant complexities involved, it has been said that "early and full cooperation in an investigation into anti-competitive conduct provides benefits of a scale and nature seldom encountered in the criminal jurisdiction".[34] A proceeding for pecuniary penalties under the Act at issue here may be less complex than some Commerce Act cases. For example, counsel for RBNZ thought that if this matter had proceeded to hearing it might have occupied a week's hearing time. But the savings to the administration of justice and the public purse extend beyond the hearing of a matter. There are also public interest factors that are relevant. Just as with other regulatory pecuniary penalties cases, there is a public interest in providing appropriate incentives to reporting entities to cooperate with the supervisor when compliance issues arise.

[53] The parties submit that, even if the discount here could have been higher than 20 per cent, it is within range. They submit that overall it is part of the compromise they have reached and it does not put the overall proposed penalty out of range. However, here I consider the starting point to be arguably on the high side. I consider the discount to be too low when compared with cases under the Act and other regulatory cases. Together, I consider the end point reached for this breach is too high.

[54] If the Court endorses it, it will set a precedent for cases that follow. That risks being unfair to those that follow. This may be all the more so for defendants of good standing, who are wanting to preserve their good reputation in the market by demonstrating full cooperation, and who may feel it necessary based on precedent to agree to a higher penalty than that which they consider is necessarily warranted.

[55] As the cases have established, there are good reasons why the Court should not embark on its own enquiry if the agreed penalty is within range. Certainly, a defendant

---

33 *Hessell v R* [2010] NZSC 135, [2011] 1 NZLR 607 at [45]-[46].

34 *Commerce Commission v EGL Inc* HC Auckland CIV-2010-404-5474, 16 December 2010 at [24]. See also *Commerce Commission v Alstom Holdings SA* [2009] NZCCLR 22 at [18].

should not be deterred from a negotiated resolution by fears that it will be rejected by the Court as too low simply because it does not coincide precisely with the penalty the Court might have imposed.[35] However, neither a defendant nor a regulator should be deterred from a negotiated resolution if the Court adjusts the agreed penalty downwards because a discrete discount the parties have agreed to in reaching their resolution is too low relative to the established approach in these or similar cases.

[56] Given TSB's full cooperation and early and complete admissions, I consider at discount of not less than 25 per cent was appropriate. Taking the agreed starting point and uplift, but applying a discount of 25 per cent to the starting point, the penalty for this breach would be $1 million (rather than $1,062,500).[36] I will consider at the end the combined effect of a 25 per cent discount for each of the breach categories to determine whether the overall end penalty agreed is out of range.

Second breach

Summary

[57] RBNZ alleges and TSB accepts that TSB breached its obligation to regularly review and maintain its AML/CFT programme. While the Act does not specify when an AML/CFT programme is to be reviewed, the parties agree that where deficiencies are identified, that should trigger a review. Here, the 2017 audit identified two key areas of non-compliance (staff training and transaction monitoring) and one area for improvement (review of policies and procedures). This did not trigger an adequate review, which meant that the identified deficiencies had not been addressed by the time of the 2019 audit. TSB also failed to meet several of its own target review dates for specific policies and procedures.

[58] The parties agree that a penalty of $1,125,000 is appropriate for TSB's breach of this obligation. They have arrived at this penalty by taking a starting point of $1.25 million. To that they propose a 10 per cent uplift because of the warning issued

---

35 *Alstom Holdings*, above, at [18]; cited in *Financial Markets Authority v ANZ Bank New Zealand Ltd*, above n 2, at [30].

36 The parties have adopted the methodology where the uplift and discount are each applied to the starting point, rather than applying the discount to the adjusted starting point (inclusive of the uplift).

by RBNZ to TSB in 2016 and TSB's knowledge of ongoing non-compliance. They then propose a 20 per cent discount to reflect TSB's admission of liability and cooperation.

Circumstances

[59] Section 59(1) of the Act requires a reporting entity to review its risk assessment and AML/CFT programme to ensure it is up to date, to identify deficiencies in its effectiveness and to make any necessary changes. This supports the general requirement in s 56 that a reporting entity "establish, implement and maintain" an AML/CFT programme. There is no timeframe for when reviews are to be carried out.[37] However, audits are required every two years and this provides an opportunity for issues to be identified and then addressed.

[60] The 2017 Deloitte report gave a qualified opinion as to TSB's compliance with its then current risk assessment and AML/CFT programme. It identified two areas of non-compliance and areas for improvement:

(a) Staff training: Deloitte identified that TSB was not actively identifying and training staff that had not completed the required training. Staff were able to complete their training assessment without reviewing the supporting material. This meant there was a risk that staff were unaware of their AML/CFT responsibilities or unaware of the AML/CFT risks faced by TSB.

(b) Transaction monitoring: Deloitte identified that TSB had not adequately designed and implemented all controls required to identify potential money laundering or financing of terrorism activities occurring within TSB's operations.

(c) Review: TSB had not reviewed the relevant policies and procedures in the two-year period prior to Deloitte's 2017 report and there was no

---

[37] Compare with *Qian DuoDuo*, above n 21, at [2], which incorrectly states that reviews are required every two years.

calendar schedule to ensure the regular review of policies and procedures.

[61] TSB's remediation and agreed action plan stated that the issues would be addressed by specified dates. One of the proposed actions was that frontline staff that had not completed their training would be prevented from processing transactions or onboarding new customers. There would be an exception for newly appointed staff, who would have 30 days to complete their compulsory training. The executive leadership team would receive a monthly report detailing non-certified staff. Payroll would also receive the monthly report to restrict non-certified staff from processing transactions or onboarding customers. The target date for this work was the second quarter of 2018.

[62] These monthly reports to the executive leadership team were provided by TSB's Head of Compliance in May, June, July, August and October 2017. The reports then ceased for reasons that are not clear. However, the timing broadly aligned with when the Head of Compliance and the Chief Risk Officer left TSB.

[63] There is no documentary evidence of any instruction to Payroll to remove access to any frontline staff who had not completed training. This had not been actioned by August 2017 when TSB's Chief Risk Officer advised the executive leadership team that there were "quite a few staff members here who have not completed their compliance training" and this was getting "really concerning". The Chief Risk Officer said they should have their ability to interact with customers removed and he would be asking the team what action they were taking to enforce compliance. TSB's internal audit partner reported to TSB's audit committee that front-line staff with outstanding training requirements would be removed from processing. There is, however, no evidence that this ever happened.

[64] TSB had a system for sending escalation reminders to the Head of Compliance concerning staff training. Escalation reminders were sent to the new Head of Compliance in June, July and September 2018. This did not prompt action apparently because they were regarded as a legacy reminder to the previous Head of Compliance and no longer relevant. This meant that the previously implemented compliance

reporting did not continue. However, a different reporting system that covered frontline staff was in place from February 2018.

[65] Also, the executive leadership team received a report from the Chief Risk Officer that training rates had improved – overall completion rates were 95 per cent in July 2017, 99 per cent in August 2017, 100 per cent in September 2017 and 97 per cent in October 2017. There is no evidence that the executive leadership team was aware that a process had not been put in place to stop system access for staff who had not completed training. All reporting to the Board indicated that issues identified by Deloitte in 2017 had been addressed.

[66] To address the 2017 Deloitte concerns regarding transaction monitoring, "sequences" of actions were proposed:

(a) Sequence 1 proposed a shift from an in-house system to a new system provided by a third-party service provider. This was approved by the executive leadership team in April 2018. The timeline for this was extended due to delays in contractual and pricing negotiations, partly because of competing business initiatives that were given priority.

(b) Sequence 2 involved a review and reconciliation of all transactions from high risk countries. This was not progressed due to lack of clarity about what was required, which was not helped by the departure of key personnel in late 2017/early 2018, confusion about whether it was impacted by the delays with sequence 1, and the understanding of some staff that the action was closed.

[67] The audit committee was aware of the delays with sequence 1 through reports in May and November 2018 and February and May 2019. The Board was not made aware of any issues with sequence 2.

[68] As to ensuring regular reviews of its AML/CFT programme, an instruction was given to document the frequency of review that was to apply. This task was allocated to a member of TSB's risk team for action by 31 December 2017. However, the matter

was closed without this happening. This was pursuant to confirmation received from the relevant risk team member that was based on insufficient evidence. There were reminder notices generated to staff of the need to review the programme, but these did not prompt a review. This seems to have been because of an internal perception that these notices were outdated or being directed to the wrong staff. All reporting to the Board and committees suggested that the issues from the 2017 Deloitte report had been addressed.

[69] The result was that, by the time of the 2019 audit, the matters of non-compliance and areas of improvement raised in the 2017 audit remained unaddressed. Reflecting this, the 2019 Deloitte report identified that:

(a) Controls established to ensure compliance with training requirements were not operating effectively to ensure that all new or existing staff in AML/CFT-related roles had completed their required training. It recommended that this occur as a high priority and that TSB suspend the ability to process transactions or onboard new customers.

(b) Exceptions with monitoring activities or failures in the design of controls meant that there was a risk that TSB was not identifying all potential money laundering or financing of terrorism activities occurring within TSB's operations.

(c) Components of the AML/CFT programme had not been updated annually, as required by TSB's risk assessment document and, while TSB had reviewed and updated its risk assessment document in 2017 and 2018, four policies had not been reviewed and updated.

[70] For some of its policies, TSB had deadlines for review. In having these deadlines it must have contemplated that over a period of time those policies might become outdated and a review should occur. However, TSB also failed to meet its own target review dates:

(a) TSB's review date for its policy for reporting suspicious or unusual transactions was by 31 December 2018. At the time of RBNZ's 2019 on-site report, this review was seven months overdue.

(b) TSB's review date for its procedure for unusual behaviour was by 22 September 2017. At the time of RBNZ's 2019 on-site report this was 22 months overdue.

(c) TSB's review date for its staff training procedure was by 31 March 2018. This was at least 16 months overdue by the time of RBNZ's 2019 on-site report.

(d) TSB's review date for its "Know Your Customer Policy" was by 31 March 2019. It was at least four months overdue by the time of RBNZ's 2019 on-site report.

(e) TSB's review date for its records management procedure was 31 March 2019. It was at least four months overdue by the time of RBNZ's 2019 on-site report.

(f) TSB's onboarding policies were scheduled to be reviewed by 31 March 2019. It was at least four months overdue by the time of RBNZ's 2019 on-site report.

(g) TSB's policies for termination of banking relationships was scheduled for a review on 31 March 2019. It was at least four months overdue by the time of RBNZ's 2019 on-site report.

[71] TSB has not been able to identify why these target dates were not met. There is no evidence that TSB's senior management or Board were aware of this.

[72] TSB accepts that it failed to maintain and review its AML/CFT programme as required by ss 56 and 59(1) of the Act because, at the time of the 2019 Deloitte report, areas of non-compliance identified in the 2017 report had not been adequately addressed or were not addressed at all. Further, TSB had failed to comply with its own

target dates for ensuring the currency of its policies that formed part of its AML/CFT programme.

Remediation and cooperation

[73] As noted earlier, following the 2019 Deloitte report, TSB took immediate steps to improve its compliance with the Act. This included remediation activities in respect of staff training, transaction monitoring and the currency of its policies. It also fully cooperated with the investigation and this proceeding.

Penalty

[74] The parties agree that the most concerning factor of this breach was that by 2019 TSB had failed to remedy the substantive issues which Deloitte had identified in 2017. This related to staff training and transaction monitoring which are core areas of concern for any AML/CFT programme.

[75] They also agree that a further serious factor was that, having identified that specific policies required review within a specified timeframe, it failed to meet those timeframes. These policies included core areas of compliance, including reporting suspicious or unusual transactions, records management and the procedure for escalation of unusual behaviour reports.

[76] The maximum penalty for this breach is $2 million.[38] As with the first breach, the parties agree that it falls within the middle of their proposed "high culpability" band and they have proposed a starting point of $1.25 million. They agree that this should be uplifted by 10 per cent for two aggravating factors. The first is that TSB ought to have prioritised its review obligations following the 2016 warning. The second is the organisational knowledge of non-compliance that the parties agree was an aspect of a systemic failure in TSB's overall approach to its review and maintenance obligations.[39] They have proposed the same 20 per cent discount for admission and cooperation.

---

38 Sections 78(f) and 90(3)(b).

39 New monthly reports regarding staff training ceased from October 2017, system generated reminders did not prompt action, priority was not given to the new monitoring systems, no clear calendar review schedule was put in place, and TSB missed its own review dates for some policies.

[77] I consider that the breach is comparable to but arguably a little more serious than the first breach. The non-compliance occurred over a shorter period but related to issues that had been brought to TSB's attention. TSB then failed to follow through on action plans, system-generated alerts, and internal review dates, which is indicative of systemic failures and which occurred despite the earlier warning. I therefore consider that an adjusted starting point of $1,375,000 is not out of range.

[78] For the reasons discussed above, I consider a discount of just 20 per cent is too low. The appropriate discount is not less than 25 per cent. With a discount at that level it would mean an end penalty for this breach of $1,062,500 (compared with the proposed $1,125,500) for this breach.

Third breach

Summary

[79] This breach concerns a failure to conduct a risk assessment of TSB's realty operations. A risk assessment is a pre-requisite for establishing an AML/CFT programme and conducting CDD. While TSB conducted CDD and established an AML/CFT programme in respect of its realty operations, it did not conduct a risk assessment of this business before doing so. The parties agree that this was a breach of s 58(1) or, alternatively, s 59(1) of the Act.

[80] The parties have agreed that a starting point of $1.25 million is appropriate for this breach. They propose a five per cent uplift because of the warning referred to earlier and a 20 per cent discount for TSB's admission of liability and cooperation. This results in a final proposed penalty of $1,062,500.

Circumstances

[81] The Department of Internal Affairs has assessed the real estate sector as a "medium-high" risk for money laundering and the financing of terrorism. From 1 January 2019 TSB was required under s 58 of the Act to have carried out a full assessment of the risk of money laundering and the financing of terrorism that it might reasonably have expected to face in its realty operations.

[82] As at 1 January 2019, TSB had a risk assessment in relation to its banking operations. This referred to its realty operations as follows:

> The Realty business will be subject to additional regulation as part of Phase 2 AML/CFT reforms and the risk of that business will be assessed fully as part of that. Discussions with the Realty team indicate that cash into the Trust accounts is prohibited. Realty staff, as bank employees are subject to TSB AML awareness training and manual reporting requirements. Therefore procedures to prevent/detect ML/TF in the Realty business are arguably tighter than comparative real estate businesses.
>
> The Realty business is solely focussed on the Taranaki region, principally New Plymouth. Comparative to the Auckland market buyers are principally New Zealand[ers] with funds originating from NZ institutions. Media articles suggest large foreign inflows of criminal proceeds to invest in real estate are less applicable to TSB's Realty business. Therefore, trends such as these buyers wanting to deposit cash would be 'unusual' for its business.

[83] TSB accepts that this was insufficient to amount to a risk assessment as required by s 58.

[84] TSB did undertake some steps in relation to its realty operations that were intended to comply with the Act. It conducted CDD, carried over aspects of its AML/CFT programme from its banking operations, developed some new processes and procedure documentation, developed training materials and delivered a training programme to realty staff and contractors, and put in place assurance and support processes. However, a risk assessment was necessary before these steps were taken.

[85] The parties agree that TSB breached s 58(1) because TSB did not conduct a risk assessment in respect of its realty operations prior to establishing an AML/CFT programme and carrying out CDD for that business. Alternatively, s 59 of the Act required TSB to review its overall risk assessment in view of the Act's application to its realty operations from 1 January 2019.[40] They agree that, either way, the nature of the breach was the same: TSB failed to conduct a risk assessment in respect of a significant and discrete part of its business.

---

[40] It failed to do so because, in respect of its realty operations, it did not have regard to the matters set out in s 58(2)(b), it failed to put its risk assessment in writing, and it failed to satisfy the requirements of s 58(3)(a) and (c).

[86] The parties agree that this occurred because priority was not given to it by TSB's risk team. This team was aware that a full risk assessment was needed for this aspect of TSB's business. It was brought further into focus in December 2018 following an external report on the adequacy of the risk assessment for its realty operations. Despite this, no work was undertaken by the risk team. This was apparently because it was thought that it would be better dealt with as part of a wider review, the terms of which it was discussing with Deloitte.

[87] All reporting to senior management, the Board and committees suggested that TSB had taken necessary steps to meet its new obligations under the Act in respect of its realty operations.

[88] Work on the risk assessment for TSB's realty operations did not commence until August 2019, after TSB became aware of the extent and seriousness of its non-compliance with s 58 of the Act.

Remediation and cooperation

[89] An updated risk assessment, which included TSB's realty operations, was completed on 31 December 2019. TSB provided this to RBNZ on 17 January 2020. RBNZ confirmed, in email correspondence on 7 July 2020, that this action was closed. As stated above, TSB fully cooperated with the investigation and proceedings.

Penalty

[90] Section 90(1) of the Act provides that the Court may order a person to pay a pecuniary penalty if the person has engaged in conduct that constituted a "civil liability act". Section 78 provides that 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 does any of the matters in s 78(a)-(g). The maximum penalties in s 90 refer to 78(a)-(g) but not to the maximum when the failure is not one of those specific matters. This means that some civil liability acts do not have specified maximum penalties.

[91] There is no specific maximum penalty for TSB's failure to conduct a risk assessment of its realty operations. The parties submit the maximum is determined with reference to the nature and importance of the civil liability act in comparison with the civil liability acts for which there are specified maximum penalties.[41] The parties consider that the failure to conduct a risk assessment for an aspect of TSB's business is comparable in seriousness to failing to update and maintain a risk assessment and the maximum of $2 million should apply.[42]

[92] The parties again propose a starting point of $1.25 million on the basis that the breach was in the middle of their suggested "high culpability" band. This is because the sector is regarded as being of medium to high risk by the DIA, a risk assessment is a fundamental first step required by the Act and there was a wholesale failure to comply with this core requirement in relation to TSB's realty operations.

[93] I consider the proposed starting point to be at the top of the available range if not a little outside that range. This was not a wholesale failure by TSB to comply with its obligations under the Act in relation to its realty operations. It was a specific failure, albeit of a key component of the Act's requirements. It was unintentional in that TSB intended to comply with its obligations and was discussing a wider review that would encompass this work. The breach related to a seven-month period rather than extending over several years and it occurred at the start of the regime as it applied to realty businesses. It is also relevant that the realty business was a relatively small part of TSB's overall operations.

[94] I consider it is arguable that this breach was not as serious as the first or second breaches. A feature of the first breach was the lengthy period over which it extended. A feature of the second breach was the specific notice of non-compliance that TSB had through the 2017 audit. In both cases, the breaches related to its (larger) banking operations where the risk to confidence in New Zealand's financial institutions from TSB's non-compliance is greater. Had I been asked to consider the starting point on a

---

41 Relying on *Ping An*, above n 25, at [85].

42 Relying on *Qian DuoDuo*, above n 21, which concerned a failure to update and maintain a risk assessment.

contested basis, I would likely have adopted a lesser starting point for this breach than that proposed by the parties.

[95] The parties are agreed that there should be an uplift because this breach occurred despite the warning. The parties agree that the warning should have led to TSB ensuring that all aspects of its business were compliant. They therefore propose an uplift of five per cent to the starting point. I have no issue with this.

[96] The parties propose a 20 per cent discount for TSB's admission and full cooperation. For the reasons discussed earlier I consider this is too light. A discount of not less than 25 per cent was appropriate. This would mean a penalty of $1 million (rather than $1,062,500) for this breach.

Fourth breach

Summary

[97] This concerns TSB's failure to have regard to certain countries with which it deals when reviewing its 2017 risk assessment for its banking operations. For this breach the parties consider that a starting point of $750,000 is appropriate. They propose a downwards adjustment of 20 per cent for TSB's admission of liability and cooperation. This would result in a final proposed penalty of $600,000.

Circumstances

[98] Section 58(1) requires that a reporting entity undertake an assessment of the risk of money laundering and the financing of terrorism that it may reasonably expect to face in the course of its business. Section 58(2)(e) requires that, in undertaking the risk assessment, the reporting entity have regard to the countries it deals with. Section 59 requires the reporting entity to review its risk assessment to ensure that it and its AML/CFT programme are up to date.

[99] The countries the reporting entity deals with are an important consideration of every risk assessment. While all countries are exposed to illicit international money flows, some are more vulnerable than others. The parties agree it is essential that a risk assessment identify the countries it deals with that do not have, or have

insufficient, AML/CFT programmes in place. The reporting entity's AML/CFT programme then needs to include additional measures to manage and monitor dealings with these countries.

[100] TSB reviewed its risk assessment for its banking operations in September 2017. In undertaking that review it failed to identify five (of the 77) countries with which it had, and was reasonably expected to continue to have, dealings.[43] This failure occurred because TSB staff did not conduct comprehensive or sufficient quarterly reviews of a countries list that supported its risk assessment process. It is accepted as unlikely that the Board, committees, and senior management were aware of this failure.

Remediation and cooperation

[101] As noted above, an updated risk assessment was completed on 31 December 2019. TSB provided this to RBNZ on 17 January 2020. RBNZ confirmed in email correspondence on 7 July 2020 that this action was closed. TSB fully cooperated with the investigation and these proceedings.

Penalty

[102] There is no specific maximum penalty for a breach of obligations relating to risk assessments. The parties submit the maximum should be $2 million as a risk assessment is the first step in establishing and reviewing an AML/CFT programme.[44] They submit this failure is in the middle of their proposed "medium" culpability band. The suggested percentage of the maximum penalty for this band is 25-50 per cent. They therefore propose a starting point of $750,000 (37.5 per cent of $2 million). They do not propose an uplift because of the warning as they see this breach as one of accuracy and completeness. They submit a discount of 20 per cent should then be applied for TSB's admission and cooperation.

---

43 Once this failure was rectified, these five countries have been included with twenty other countries of highest risk.

44 They refer to the analysis at [90] and [91] above.

[103] I consider the starting point to be at the high end. If the parties did not have any AML/CFT programme and this was intentional and inexplicable the maximum penalty would be $2 million. Here, TSB did have a risk assessment that had regard to the various items specified in s 58(2). It did have regard to most of the countries with which it has dealings but overlooked five countries. A penalty at 37.5 per cent of the maximum seems high relative to the highest culpability in this kind of case.

[104] That said, because TSB plays a critical function in New Zealand's economy as a registered bank and is far larger than most reporting entities under the Act, a starting point of 37.5 per cent may not be out of range, but it would be at the high end of the appropriate range. For the reasons discussed earlier, I consider that a discount of not less than 25 per cent was appropriate for TSB's admission and cooperation. This means an end penalty of $562,500 (rather than the proposed $600,000 for this breach).

Overall assessment

[105] The parties submit that the four breaches concern discrete conduct. There has been no double counting. They have compared the total proposed penalty with other cases under the Act. Three of them concerned more serious breaches, but by smaller entities, where cumulative starting points were $4.8 million, $4.1 million, and $3.9 million and $2.7 million (two defendants in one case) respectively.[45] The fourth involved a moderately sized business and civil liability acts at the lower end of seriousness. The Court imposed a starting point of $420,000.[46]

[106] Perhaps the better comparison is with the starting points in those cases that concerned breaches relating to deficient or non-existent risk assessments and AML/CFT programmes. In *OTT* one of the defendants had a deficient AML/CFT programme based on inadequate risk assessments and the other did not have an AML/CFT programme at all. The Court adopted a starting point of $650,000 and $1.5 million respectively.[47] In *Qian DuoDuo* a starting point of $225,000 was adopted for an inadequate risk assessment.[48] In *Jin Yuan Finance*, the AML/CFT programme

---

45 *Ping An*, above n 25; *Jin Yuan*, above n 24; and *OTT*, above n 25.
46 *Qian DuoDuo*, above n 21.
47 *OTT*, above n 25, at [57] and [60].
48 *Qian DuoDuo*, above n 21 at [145].

continued to be deficient despite a formal warning. It is unclear why there was no separate starting point for this breach but it may explained by the multiplicity of breaches which led to an overall starting point of $4.1 million and a 15 per cent uplift for misleading behaviour.

[107] A comparison with these cases confirms my view that the agreed starting points here for the four breaches are at the high end. Largely they can only be justified by the position that TSB occupies in New Zealand's economy as a registered bank (even though TSB is not one of the largest banks and has a different ownership structure and so did not gain financially from the conduct). While some of the breaches extended over a long period and TSB was on notice in respect of some of them and failed to take timely action to remedy them, but that was also the position in three of the cases under the Act.[49] When the overall high starting points (which may have been within range but at the high end) are combined with the unduly low discount for mitigating factors I consider the agreed overall penalty is a little outside the appropriate range.

[108] I acknowledge that the agreed position reached between the parties would have involved compromises on each side. However, this judgment will provide a precedent for negotiations between supervisors and reporting entities who breach their obligations in the future. If 20 per cent is upheld here as within range for full cooperation and early admission, other reporting entities, who wish to show full cooperation by presenting agreed penalties to the Court, may find it difficult to negotiate a higher discount. The Court should be careful not to endorse a penalty that will operate unfairly on others who come to the Court.

[109] If the only adjustment is made to the discount, the overall penalty should be $3,625,000, comprising:

(a) $1 million for the first breach;

(b) $1,062,500 for the second breach;

(c) $1 million for the third breach; and

---

[49] *Ping An*, above n 25; *Jin Yuan*, above n 24; and *OTT*, above n 25.

(d) $562,500 for the fourth breach.

[110] Given my view that all of the starting points are at the high end, standing back and assessing the conduct as a whole, I consider a small totality adjustment should be made. I consider this adjustment should be made to the third breach. I reduce that to $875,000 which brings the overall penalty to $3.5 million.

Result

[111] I impose a penalty of $3.5 million on TSB for the admitted breaches of the Act which is made up of $1 million for the first breach, $1,062,500 for the second breach, $875,000 for the third breach and $562,500 for the fourth breach.

Mallon J