IN THE HIGH COURT OF NEW ZEALAND
AUCKLAND REGISTRY

I TE KŌTI MATUA O AOTEAROA
TĀMAKI MAKAURAU ROHE

CIV-2019-404-1714
[2020] NZHC 1663

BETWEEN	THE DEPARTMENT OF INTERNAL AFFAIRS Plaintiff
AND	OTT TRADING GROUP LIMITED First Defendant
	TONGHUI QI Second Defendant
	LEE CHON WOON Third Defendant

Hearing: On the papers

Appearances: D J Johnson / S McMullan for Plaintiff
No appearance for First and Fourth Defendants

Judgment: 10 July 2020

JUDGMENT OF LANG J
[on application for pecuniary penalty orders]

This judgment was delivered by me on 10 July 2020 at 3.30 pm, pursuant to Rule 11.5 of the High Court Rules.

Registrar/Deputy Registrar

Date……

Solicitors:
Meredith Connell, Auckland

[1] In this proceeding the Department of Internal Affairs (the Department) alleges that, between May 2014 and April 2019, OTT Trading Group (OTT) and MSI Group Limited (MSI) breached their obligations under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (the Act). The Department commenced this proceeding seeking injunctions against OTT and MSI, as well as their sole directors and shareholders, Mr Qi and Ms Duan. It also sought orders against Ms Woon, who was OTT's compliance officer between February 2017 and April 2019. Her role was to ensure OTT complied with the requirements of the Act.

[2] In a judgment delivered on 15 May 2020 I recorded the terms on which all defendants other than OTT and MSI had agreed to settle the proceeding.[1] OTT and MSI have never taken steps to oppose the application. Furthermore, the remaining defendants, all of whom were associated with either OTT or MSI, acknowledged in a statement of agreed facts that both companies had breached their obligations under the Act. The Department now seeks judgment by way of formal proof against both corporate entities. In particular, it seeks both a civil pecuniary penalty and injunctions restraining each company from carrying out any financial activity in the future that would cause it to be deemed a reporting entity under the Act.

The AMF/CFT regime – a brief overview

[3] The Act establishes a regime for the detection and prevention of money laundering and for the purpose of countering the financing of terrorism (AML/CFT). The purposes of the Act are as follows:[2]

> (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.

---

1 *Department of Internal Affairs v OTT Trading Group Ltd* [2020] NZHC 1005.
2 Anti-Money Laundering and Countering Financing of Terrorism Act 2009, s 3(1).

[4] The Act came into full force on 30 June 2013. From that date, all persons or entitles meeting the definition of "financial institution" are deemed to be "reporting entities" for the purposes of the Act. A financial institution is an entity that carries on any activity that includes among other things:[3]

(a) Transferring money or value for, or on behalf of, a customer; or

(b) Money or currency changing.

[5] The Act imposes obligations on reporting entities. In *Department of Internal Affairs v Ping An Finance (Group) New Zealand Company Ltd* (*Ping An*) Toogood J summarised these as follows:[4]

> (a) Subpart 1 addresses customer due diligence obligations which must be observed before a reporting entity can carry out a transaction for that customer, prescribing a hierarchy of standards (simplified, standard and enhanced) depending on the nature and circumstances of the customer
>
> (b) Subpart 2 places a statutory duty on a reporting entity to convey to the Commission of Police information that comes to its attention in respect of which it has reasonable grounds to suspect it may be relevant to the investigation of prosecution of money laundering, or 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.
>
> (c) Subpart 3 specifies that reporting entities must keep records relating to every transaction, with strict requirements of details to allow the ready reconstruction of transactions and the identification and verification of the persons involved.
>
> (d) Subpart 4 provides that every reporting entity must have a compliance programme and a compliance officer and sets minimum standards for such programmes.

[6] Every reporting entity must have an AML/CFT programme.[5] The programme, and its related risk assessment, are foundational aspects of the Act. It is the repository for the entity's internal procedures, policies and controls relating to detecting money laundering and countering the financing of terrorism. The AML/CFT programme must reflect the entity's own risk assessment, which in turn is based on an

---

3 Section 5.

4 *Department of Internal Affairs v Ping An Finance (Group) New Zealand Company Ltd* [2017] NZHC 2363, [2018] 2 NZLR 552 at [21] [*Ping An*].

5 Section 56. The minimum requirements are set out in s 57.

identification of the risks the entity may reasonably expect to face in the course of its business.[6] The assessment must also describe how the entity proposes to ensure the assessment remains current.

[7] The Act also requires entities to conduct due diligence regarding the clients on whose behalf they conduct business. This is based on the proposition that entities must know who their customers are. Entities must therefore conduct due diligence on its customers when they enter into a business relationship with them, or when a customer seeks to conduct an occasional transaction.[7] If an entity cannot conduct customer due diligence as required, it must not carry out an occasional transaction nor enter into a business relationship with a customer.[8]

[8] The extent of due diligence required depends on the risk posed by the customer, or by the transaction. Standard customer due diligence requires the entity to obtain verified information about the customer's identity, the nature and purpose of the proposed business relationship, as well as sufficient information to determine whether the customer should be subject to enhanced customer due diligence. Enhanced due diligence is required whenever a customer seeks to conduct a complex or unusually large transaction,[9] or when there is an unusual pattern of transactions without an apparent or visible economic or lawful purpose.[10] In addition to the standard due diligence requirements, the Act requires the entity to obtain verified information relating to the source of the customer's funds or wealth.[11]

[9] Reporting entities must also monitor their accounts.[12] They must continue to ensure the information the customer provided initially continues to match its activities and transaction behaviour. To discharge this obligation, reporting entities must have a system in place to identify patterns of transactions that raise a suspicion of money laundering or financing of terrorism.

---

6 The minimum requirements for the risk assessment are set out in s 58(3).
7 Section 14.
8 Section 37.
9 For money transmitters of this size any transactions over $50,000 in value will be generally be considered unusually large: *Ping An*, above n 4, at [35].
10 Section 22(1).
11 Sections 23(1)(a) and 24(1).
12 Section 31.

[10] Reporting entities must also maintain adequate records for at least five years.[13] Reports of suspicious activity, records of identity verification and other specified records must also be kept for at least five years.[14]

Facts

[11] MSI and OTT are two members of a group of entities that provided money remittance and foreign exchange services within New Zealand and Australia. The group began operating in October 2001, when Wisdom Financial International Co Ltd (Wisdom) was incorporated. Mr Li was its sole director and shareholder. Wisdom also employed Ms Duan and Mr Qi. In 2012, Wisdom transferred a substantial portion of its business to MSI Financial Ltd (MSI Financial). MSI Financial was wholly owned by Ms Duan, and it employed Mr Qi. MSI Financial operated out of premises in central Auckland.

[12] MSI was incorporated on 29 May 2014 to provide financial services in Christchurch. It was never registered as a financial services provider, and at no stage submitted an annual report. MSI undertook or processed at least $213 million in transactions.

[13] OTT was incorporated on 20 November 2014 and registered as a financial services provider on 9 January 2015. At all material times, Mr Qi was its director and shareholder. Between 2015 and 2019 OTT processed at least $196 million in customer transactions. More than a third of these in terms of value engaged the enhanced due diligence requirements of the Act.

[14] On 28 August 2014, a compliance officer from the Department, Mr Milnes, visited MSI Financial's offices in Auckland. There he spoke with Ms Yu, the company's compliance officer. She confirmed that MSI Financial maintained an AML/CFT risk assessment and a compliance programme, both of which had been prepared by "AML Solutions". In January 2015 the Department commenced a desk-based review of MSI Financial's compliance with the Act. On 27 January, MSI

---

13 Section 49.
14 Sections 49A, 50 and 51.

Financial sent the Department copies of its AML/CFT risk assessment, and its compliance programme. Those documents were both dated July 2013.

[15] MSI Financial reported that it operated from its Auckland premises. Two days later MSI Financial informed the Department that it planned to cease offering financial services as of 31 March 2015. It did not tell the Department that it planned to transfer its business to MSI and OTT, or that it had any connection with those entities. This advice caused the Department to discontinue its review of MSI Financial's activities.

OTT

[16] On 24 February 2015, the Department contacted OTT enquiring about the nature of its business operations. The Department was not aware at that time of any connection between MSI Financial and OTT. In response, Mr Tonghui Qi sent the Department an email attaching a compliance programme in the form of a slideshow, together with a blank document purporting to be a risk management assessment.

[17] On 1 April 2015, Mr Milnes went to OTT's premises in Mount Albert. Whilst there he spoke to Mr Qi, and observed material relating to MSI Financial. Mr Qi said that OTT was his company although he had also worked for MSI Financial for 10 years and still worked for that company. He said OTT intended to provide both financial advice and currency exchange services.

[18] Mr Milnes told Mr Qi he was under the impression MSI Financial had ceased trading. This prompted Mr Qi to begin a lengthy telephone conversation in Mandarin with an unknown individual. Afterwards, Mr Qi told Mr Milnes that OTT was set up to open a bank account in its own name for the benefit of MSI Financial, and that MSI Financial had stopped providing services to its clients. He also said he did not know whether OTT had an AML/CFT programme, and that it had no employees.

[19] The following day a member of the Department's Financial Integrity Unit wrote to OTT, informing it that the Department would be conducting a review of OTT's AML/CFT compliance programme. On 24 April 2015 he received a response from OTT that attached a certificate awarded to Mr Qi for his completion of a AML/CFT training session, an AMF/CFT compliance programme, and a risk

assessment. The latter two documents were virtually identical to the documents supplied earlier by MSI Financial. The Department sent OTT a letter noting the resemblance, and requesting more information about the relationship between the two entities.

[20] On 22 May 2015, Mr Milnes received an email from OTT's email address. This explained that Ms Duan had decided to cease MSI Financial's Auckland operations, and that OTT had been incorporated so Mr Qi could take over MSI Financial's operations. The email also stated that Ms Duan had agreed to transfer MSI Financial's clients and databases to OTT, and that OTT had adopted MSI Financial's risk assessment and compliance programme. The email confirmed that OTT did not operate from MSI Financial's former premises in central Auckland.

[21] Mr Qi did not mention that Ms Duan was the person who had incorporated MSI and that it was providing money remittance services in Christchurch.

[22] On 24 July 2015 the Department conducted a desk-based review of OTT's risk assessment and compliance programme. This found that OTT's programmes appeared compliant with the Act. That assessment changed following a more intensive assessment of OTT's business operations and regulatory compliance. As it transpired, OTT had not put into place its risk assessment procedures, and its practices were inadequate or non-existent in terms of due diligence and recordkeeping.

[23] On 7 October 2015, OTT changed its registered address to MSI Financial's former address in central Auckland. Mr Milnes and another compliance officer, Mr Holmes, visited OTT's premises the following month. During this visit they were told OTT had 5 employees, each of whom had previously worked for other entities in the group. Three employees had previously been employed by MSI Financial. The Department also discovered OTT held no records relating to its business activities prior to 1 October 2015.

[24] Mr Milnes and Mr Holmes spoke with OTT's employees. They said OTT had been operating in a different manner to that described in the company's risk assessment because it operated as a money remitter using an informal system of funds

transfer. They also said the company maintained additional bank accounts that were not disclosed on its risk assessment. Mr Li, an employee, told the officers that OTT had taken over MSI Financial's customer database, and that Ms Duan had taken all information relating to MSI Financial's previous transactions with her to Christchurch.

[25] The following day, Mr Milnes issued a notice to OTT requiring it to provide all AML/CFT risk assessments and compliance programmes, as well as a copy of any written agreement relating to OTT's takeover of MSI Financial.

[26] After being informed that OTT's records were now available for review, Mr Milnes returned to OTT's premises on 24 November 2015 to conduct another inspection. Many of the records he viewed there indicated that the provider of the financial services was MSI Financial, or Morgan Stamford. No records relating to customer due diligence were available.

[27] On 26 November 2015 the Department issued a second notice to OTT requiring it to produce various records including due diligence records relating to some of the transactions it had undertaken. In response, OTT provided documentation indicating it had carried out limited due diligence on those transactions. It had not carried out any enhanced customer due diligence even though some of the transactions involved sums greater than $50,000.

[28] On 3 February 2016, the Department issued a formal warning to OTT requiring it to rectify identified areas of non-compliance. OTT responded a month later, stating that it was working to rectify the identified shortcomings. On 29 July 2016, OTT emailed the Department stating that Mr Qi would return the following week to resume his role as OTT's AML/CFT compliance officer. However, Mr Qi had returned to New Zealand nine days earlier, on 20 July 2016.

[29] On 26 September 2016, OTT submitted its 2016 annual report. It disclosed that it had one physical location in Auckland, and no other locations or subsidiaries.

[30] On 26 September 2017, OTT submitted its 2017 annual report. It declared one physical location in Auckland and one subsidiary.

[31] On 2 November 2017, the Department informed OTT that it would be conducting another on-site inspection. It issued a notice requesting certain documents in advance. OTT provided its 2017 risk assessment, which disclosed for the first time that it had acquired MSI Financial in October 2015. It also disclosed that OTT had a customer due diligence agency agreement with MSI that had been formalised in 2015, and that MSI offered its services exclusively to OTT.

[32] The Department conducted its third on-site assessment of OTT on 28 February 2018. During the inspection, the Department uplifted records relating to a sample of transactions undertaken by OTT.[15] Officers also interviewed Ms Woon, the compliance officer, about her understanding of her role. She said she had been responsible for oversight of OTT's regulatory compliance since March 2017. She said OTT had taken over MSI in April or May 2017 because it was simpler for reporting purposes to operate through one company. She said OTT's main business was the transfer of international funds, and that most of its customers were based in Christchurch.

[33] Ms Woon also said OTT was responsible for checking and verifying details sent by MSI. She said she did not know which of OTT's risk assessments was the current version, and confirmed she did not keep a record of her own or other staff members' training. She said she may have read OTT's AML/CFT programme when she started with OTT, but that she had not personally updated or amended OTT's risk assessment or the programme. She said she did not have any knowledge of the UNSC and AFAC lists referred to in OTT's AML/CFT programme.[16]

[34] Ms Woon acknowledged she was effectively incapable of acting as a compliance officer. She did not know of the circumstances in which OTT would be required to undertake enhanced due diligence. Nor could she explain the risk methodology used to measure OTT's money laundering or terrorism funding risk.

---

15 The Department takes sample transactions as it is not possible for it to interrogate every file held by a reporting entity. The Department treats samples as representative of overall compliance with the Act. OTT and MSI have had opportunities to respond and contend that the samples are not representative, but have not done so.

16 The UNSC and OFAC lists are lists of sanctioned individuals published by the United Nations Security Council and the United States Office of Foreign Assets Control.

[35] The Department completed its report following the third inspection on 1 May 2018. The report revealed that, whilst OTT frequently recorded documentation of its clients' identities, it would not investigate the source of clients' funds. This was the case even for larger transactions. In one case, it appeared that nobody from OTT had even met one of the clients, despite the total value of transactions undertaken by that client exceeding $2.5 million.

[36] On 7 May 2018, Ms Woon sent a letter to the Department attaching examples from various client files relating to the 2018 OTT sample transactions as well as other files. Ms Woon had selected these to demonstrate how OTT carried out enhanced due diligence. However, these records also indicated a failure to meet the requirements of the Act.

[37] The Department conducted its fourth and final on-site inspection of OTT on 5 January 2019. Compliance officers again spoke with Ms Woon, who confirmed OTT had not carried out enhanced customer due diligence until June 2018. She also said it had no policy, procedure or control to ensure transactions were in line with OTT's knowledge of customers and their risk profiles. Ms Woon also confirmed she did not carry out any internal AML/CFT audits. Instead, she would review a daily transaction log for sample transactions.

[38] The compliance officers questioned Ms Woon about a client who had undertaken a series of transactions involving a few thousand dollars, followed by a single transaction for $174,000. She could not provide any evidence that she had spoken to this customer, or that she had filed a suspicious activity report for the transaction. Nor could she explain why the documents attached to her letter dated 7 May 2018 did not meet the enhanced due diligence requirements under the Act.

MSI

[39] MSI has never submitted an annual AML/CFT report.

[40] The Department learned of MSI's existence in late 2016. On 12 September 2016, representatives of the Department went to MSI's premises in Christchurch. There they spoke with Ms Duan. She told them MSI was a branch of OTT, but said

there was no written agreement between them. The relationship between the two entities was instead based on a verbal agreement. She told them OTT paid the wages of MSI's staff.

[41] Ms Duan said neither MSI nor OTT had any bank account in China. She said that MSI undertook no standard procedure when it established a new business relationship with a client, and it held no records prior to September 2015 because of a systems update. Ms Duan said all MSI transactions were processed through OTT's bank accounts, and that MSI and OTT shared a common platform for managing transaction records.

[42] On 30 September 2016, the Department advised MSI that it was a reporting entity for the purposes of the Act, and was required to register as a financial services provider immediately. It was also required to provide the Department with copies of its AML/CFT programme, its risk assessment, and its AML/CFT policies and procedures. MSI did not respond to this advice, although this appears to be because the email from the Department was sent to the wrong email address.

[43] On 30 January 2017 the Department sent another email to MSI requesting documentation. Ms Duan responded on 10 February 2017, stating that MSI operated only as an agent for OTT, and that it did not provide financial services. She said she had received advice that MSI did not need to be registered as a financial services provider and did not require a separate AML/CFT programme. She also attached copies of an agency agreement between MSI and OTT as well as OTT's AML/CFT programme.

[44] On 7 September 2017, officers from the Department conducted an on-site inspection of MSI's premises in Christchurch. They spoke with Ms Duan, who told them MSI had been wound up and its business transferred to OTT in April or May 2017. She said MSI had approximately 2,000 customers, and that it advertised regularly in Chinese language newspapers in New Zealand. She said the company's principal business had been the conversion of New Zealand currency into Chinese currency. She said that some customers brought cash to MSI's premises, whilst others

transferred funds to MSI's bank accounts. She said MSI made these accounts available to OTT, and OTT carried out the currency conversions.

[45] Ms Duan told the Department that MSI did not have a compliance programme prior to April or May 2017 and that it did not maintain a risk assessment. She also said MSI was not a registered company. When confronted with MSI's active entry on the Companies Register, she said she had asked OTT to deregister MSI.

[46] Officers from the Department conducted a second on-site inspection of MSI's premises on 5 April 2019. During this inspection Ms Duan told them MSI utilised OTT's risk assessment and AML/CFT programme. She said MSI was a foreign exchange company that only engaged in transactions between China and New Zealand, and that MSI and OTT used the same foreign exchange provider. She also said that OTT processed all transactions under $50,000 and the foreign exchange provider processed the rest. She said she incorporated MSI because Mr Li could not secure bank accounts for Wisdom, and that she did what she was told by OTT.

[47] Ms Duan also disclosed that MSI had 100 to 200 regular customers, and approximately 2,000 customers in total. She said that prior to July 2018 MSI did not ask customers to provide evidence of the source of their funds, and that it did not undertake account monitoring. Ms Duan said MSI's customers were not comfortable with providing enhanced due diligence information, and that if MSI pushed for that information it risked losing business to its competitors.

[48] During the inspection, the inspecting officer took a sample of MSI's transactions. The majority of sampled transactions had not been subject to enhanced due diligence, and many lacked any verification of the customer's identity. MSI had begun to deal with many of the customers sampled after 18 July 2018, when Ms Duan claimed it started carrying out enhanced due diligence.

The civil pecuniary penalty regime

[49] The Department seeks both civil pecuniary penalties and injunctive relief against MSI and OTT.

[50] A civil liability act occurs when a reporting entity fails to comply with any of the AML/CFT requirements.[17] The Department alleges four causes of action that it says warrant the imposition of civil pecuniary penalties against MSI and OTT:

(a) Failure to establish, implement or maintain an AML/CFT programme - maximum penalty $2 million;[18]

(b) Failure to conduct customer due diligence - maximum penalty $2 million;[19]

(c) Failure to adequate monitor accounts and transactions - maximum penalty $1 million;[20]

(d) Failure to keep records - maximum penalty $2 million.[21]

[51] To determine the appropriate quantum, the Court must:[22]

(a) Assess the seriousness of the civil liability acts in order to set a starting point based on the seriousness of the non-compliance and the aggravating and mitigating factors relating to it;

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

(c) Deduct from the starting point any admission of liability or co-operation with the authorities

(d) Step back from the penalty and undertake a totality assessment by looking at the number of separate breaches to ensure there is no overlap

---

17 Section 78.
18 Sections 78(f) and 90(3).
19 Sections 78(a) and 90(3).
20 Sections 78(b) and 90(2).
21 Sections 78(e) and 90(3).
22 *Ping An*, above n 3, at [88].

between the penalties imposed for different types of non-compliance, and whether the total penalty imposed fairly and adequately reflects the overall extent of non-compliance

[52] It is also relevant to assess:[23]

(a) The extent to which the conduct was initiated or condoned by officers or senior management of the entity; and

(b) Whether steps were taken to ensure compliance with the Act including policies and step to educate officers and employees.

Failure to establish, implement or maintain an AML/CFT programme

OTT

[53] OTT consistently failed to meet the requirements of the Act. The failures were throughout almost every aspect of the AML/CFT regime. They are necessarily interlinked; a failure to collect transaction records will lead to connected failures in due diligence and programme implementation. Accordingly, the Department views these issues discretely as stand-alone civil liability acts. Its submissions therefore instead focus on the deficiencies of OTT's programme.

[54] The inadequacy of OTT's programme was in part caused by deficient risk assessments. The 2015 risk assessment failed to reflect that OTT was operating an informal system of funds transfer. Whilst this in itself is not prohibited, it does create a significant risk of utilisation of the service for money laundering or the financing of terrorism, as the funds do not go through the formal banking system.

[55] Similarly, the 2018 risk assessment did not address the process or policy behind a large volume of high value transactions to or from Australia. The failure of the programme to recognise or respond to these risks was a significant breach of the Act. The Department had notified OTT of the deficiencies in its programme as early as

---

[23] *Department of Internal Affiars v Qian DuoDuo Ltd* [2018] NZHC 1887 at [27]–[28].

December 2015. OTT took no steps to rectify the deficiencies identified by the Department.

[56] OTT's AML/CFT programme was not appropriately implemented. Key areas of implementation failure included customer due diligence, transaction monitoring, and record keeping. I address these under other heads of liability.

[57] The Department submits that a starting point of $650,000, or 33 per cent of the maximum, is appropriate. I agree. The breaches occurred over a prolonged period in circumstances where OTT was operating in a reasonably substantial way. There are no mitigating factors. OTT's actions in failing to adopt a compliant programme, despite early knowledge of its deficiencies, suggests the company had no regard for its regulatory obligations. This attitude appears to have been condoned by senior management.

MSI

[58] Throughout its interactions with the Department, MSI made varying representations about its compliance programme. In 2017, Ms Duan told the Department that MSI was a part of OTT. In 2019 she told the Department that MSI used OTT's risk assessment and AML/CFT programme.

[59] MSI had no written policies or procedures to enable compliant customer due diligence, transaction monitoring, or record keeping.

[60] The Department submits that a starting point of $1.5 million, or 75 per cent of the available maximum, is appropriate. Given that this company also operated for a prolonged period and in a reasonably substantial way I accept a significant starting point is required. There are no mitigating factors. I consider a starting point of $1.5 million under this head is warranted.

Failure to conduct customer due diligence

[61] Due diligence is central to the AML/CFT regime. An entity is required to know who its customers are, and why that customer wants to either form a business

relationship or conduct a transaction. It is only through due diligence that the AML/CFT regime is able to safeguard New Zealand's reputation in financial communities.

OTT

[62] OTT's breaches in this respect are serious. It regularly failed to conduct even standard customer due diligence. This is aggravated by its failure to undertake enhanced due diligence on relevant transactions totalling more than $60 million.

[63] Furthermore, OTT's employees seemingly failed to comprehend what was required for customer due diligence at either standard or enhanced levels. Ms Woon, OTT's compliance officer, was unable to even explain the circumstances in which enhanced due diligence was required. OTT's failure to appoint a competent compliance officer, or to implement adequate controls to ensure that customer due diligence was competently undertaken, amount to serious breaches of the requirements of the Act.

[64] Ms Woon also indicated that OTT did not collect enhanced customer due diligence before June 2018. The records for accounts since then demonstrate little improvement.

[65] Of the files submitted to or examined by the Department, there was not a single instance of compliance with enhanced customer due diligence when that was required. There is therefore no reason to believe OTT has ever undertaken enhanced customer due diligence. This is a matter of significant concern because the enhanced due diligence requirements relate to transactions for which enhanced scrutiny is appropriate. This is further aggravated by the significant volume of transactions, totalling at least $196 million, undertaken by OTT.

[66] The investigation undertaken by the Department demonstrate a complete disregard by OTT towards its compliance obligations. I consider a starting point under this head of $1.3 million, or 65 per cent of the maximum penalty, to be appropriate.

MSI

[67] MSI's breaches are aggravated by their duration and extent. There are no mitigating factors. Because MSI never submitted an annual report, it is difficult to determine what proportion of transactions were subject to enhanced customer due diligence requirements. However, based on available information between September 2015 and March 2019, at least 746 transactions undertaken by MSI exceeded the threshold of $50,000. The aggregate value of those transactions alone was $213 million.

[68] MSI generally attempted to obtain basic identity information and evidence. However, it completely ignored its obligations relating to enhanced customer due diligence.

[69] MSI's breaches of its due diligence obligations are therefore serious. Ms Duan's admission that MSI did not seek information required for enhanced due diligence out of a fear of losing customers is particularly concerning. It suggests a conscious decision not to comply with the regulatory regime for fear of the financial consequences that would follow. Such conduct requires the imposition of a stern penalty.

[70] I consider the Department's suggested starting point of $1.4 million, or 70 per cent of the available maximum, to be appropriate. The greater volume of MSI's transactions, together with the brazen nature of the breaches, justifies a higher starting point than that selected for OTT.

Failure to adequate monitor accounts and transactions

OTT

[71] The obligation to adequately monitor accounts and transactions is central to the Act. It ensures that suspicious activity is identified. OTT failed to obtain sufficient information about its clients throughout. There is thus some obvious overlap between this omission and others for which OTT is liable. However, irrespective of OTT's other failures, OTT never implemented an account monitoring policy.

[72] The Department submits that a starting point of $500,000, or 50 per cent of the maximum, is appropriate. It submits that this is appropriate when considered alongside the penalties imposed in the *Ping An* case.[24] In that case, the entity had kept no records at all and a starting point of $500,000 was selected. However, the Department submits that because OTT's conduct went for a longer period of time, the same starting point is warranted.

[73] I take a slightly different view. Although its systems were inadequate, OTT at least adopted the practice of regularly reviewing transactions. I consider a starting point of 25 per cent, or $250,000, to be appropriate.

MSI

[74] By its own admission MSI undertook no account monitoring at all notwithstanding the fact that it had 100 to 200 regular customers. It therefore totally failed to comply with this aspect of the regime. The Department submits a starting point of $500,000, or 50 per cent of the available maximum. I agree with this assessment.

Failure to keep records

[75] The obligation to maintain records is necessary for the discharge of the other obligations under the Act. It is an essential part of the AML/CFT regime. It is also necessary to enable effective investigations to be undertaken to monitor compliance. Any failure to keep records obviously undermines the objectives of the entire AML/CFT regime.

[76] There is a preliminary issue in this context. The Department submits that reporting entities must maintain records in such a way as to enable them to be viewed either immediately, or upon request. It submits that this interpretation gives the AML/CFT scheme coherence. It draws attention to s 49, which states that the records that must be kept are those that "enable the transaction to be readily reconstructed". Further, it draws attention to s 52, which provides that records must be kept in written

---

[24] *Ping An*, above n 4.

form in English, or so as to enable the records to be readily accessible and readily convertible into written form in English.

[77] The Department submits that its position is consistent with the parts of the Act relating to supervisors' monitoring of reporting entities. In particular, that the Act empowers supervisors to require the production of records and undertake on-site inspections. During inspections, supervisors may require employees to answer questions relating to the records and documents. If records were able to be held in a form not immediately accessible, then supervisors' on-site inspection powers would be significantly curtailed.

[78] I accept the Department's submissions on these issues. Any other interpretation would severely hamper the Department's ability to monitor compliance with other aspects of the regime.

OTT

[79] On multiple occasions, OTT was unable to immediately provide the Department with the records requested. In November 2015, for example, the Department was told no records were available from prior to 1 October 2015. That has proved to be the case.

[80] There is inevitable overlap under this head with OTT's failures under the other heads of liability. However, OTT's breaches were still serious; records from 2015 have never been made available.

[81] The Department submits that a starting point of $500,000, or 25 per cent of the available maximum, is appropriate. I agree with that assessment. This reflects the fact that there is a degree of overlap with breaches of other obligations. It also recognises OTT did not totally fail to keep the records required under the Act.

MSI

[82] The Department's ability to gain an accurate understanding of the role played by MSI and the transactions that it undertook was significantly hampered by the poor

record keeping systems maintained by MSI and associated companies. Like OTT, MSI was unable to produce any records for the period prior to September 2015. There is some overlap, however, between this breach and the breach of MSI's obligation to obtain sufficient customer identity information. The Department therefore suggests the same starting point as that for OTT, namely $500,000 or 25 per cent of the available maximum. Again, I accept that assessment.

Overall starting points

OTT

[83] This means I have applied the following starting points for the breaches proved against OTT:

(a) Failure to establish, implement or maintain an AML/CFT programme - $650,000.

(b) Failure to conduct customer due diligence - $1.3 million.

(c) Failure to adequately monitor accounts and transactions - $250,000.

(d) Failure to keep records - $500,000.

[84] This results in an overall starting point of $2.7 million.

MSI

(a) Failure to establish, implement or maintain an AML/CFT programme - $1.5 million.

(b) Failure to conduct customer due diligence - $1.4 million.

(c) Failure to ade1quately monitor accounts and transactions - $500,000.

(d) Failure to keep adequate records - $500,000.

[85] This results in an overall starting point of $3.9 million.

Aggravating and mitigating factors

[86] The aggravating and mitigating factors specific to the entity which may justify increasing or decreasing the penalty include:[25]

(a) Whether the entity has previously been found by a Court to have engaged in similar conduct; and

(b) Whether there has been full and frank disclosure and cooperation with the Department.

OTT

[87] OTT has not previously been found by a Court to have engaged in similar conduct. However, considering the prolonged nature of OTT's conduct, and the relative infancy of the Act, I consider its lack of any real track record to be a neutral factor.

[88] The Department submits that OTT's dealings with the Department aggravate its conduct. It submits that OTT failed to cooperate with the Department, and that it intentionally misled the Department in relation to MSI and OTT's relationship with MSI Financial. In particular, OTT was not candid about the fact that it had continued the business of MSI Financial. This, the Department says, had the effect of obstructing the Department's investigation and concealing the existence of MSI.

[89] Additionally, the relationship between MSI and OTT was characterised in different ways based on the potential advantage to the group. It was classified at different times as being that of principal/agent, parent/subsidiary and headquarters/branch.

[90] OTT's misleading conduct included excluding and providing copies of a false agency agreement, reporting that MSI was a "NZ branch/subsidiary" and an "agent"

---

25 *Ping An*, above n 4, at [102] and [119]–[125].

in its 2017 risk assessment, and Ms Woon's letter to the Department on 7 May 2018 in which she falsely stated that MSI had ceased to operate as of March 2017. The Department considers OTT's false representations were calculated to compartmentalise regulatory risk and minimise regulatory burden. The Department submits that an uplift in line with that applied in *Ping An*, namely 15 per cent, is appropriate.

[91] As Toogood J observed in *Ping An*, "efforts to frustrate the AML/CFT supervisors in their enforcement role must be met with a stern rebuke".[26] I am satisfied that OTT's conduct justifies an uplift of around 15 per cent. I therefore consider an increase of $400,000 is required to reflect this factor. This brings the overall penalty to $3.1 million.

MSI

[92] Like OTT, MSI Group has not been found by a court to have engaged in similar conduct in the past but I regard this as a neutral factor because its activities have not previously been investigated.

[93] The Department points out that MSI Group assisted OTT to mislead the Department by disguising the ongoing relationship between OTT, MSI Financial and MSI Group. The failure of MSI Group to register as a financial services provider also enabled it to remain under the Department's radar for a considerable period.

[94] The Department was not aware of the existence of MSI Group for a period of approximately 18 months after it had ceased its investigation into MSI Financial. When the Department subsequently began to investigate the activities of MSI Group, it purported to wind its activities down. In reality, however, it continued to operate until April 2019 when the department visited its offices on the second occasion. MSI Group therefore followed OTT's example of compartmentalising regulatory risk and seeking to limit the scope of the Department's enquiries.

---

[26] *Ping An,* above n 4, at [124].

[95] Furthermore, MSI Group took steps to disguise its status as a reporting entity. Ms Duan led the Department to believe MSI Group was either a branch, subsidiary or agent of OTT rather than a reporting entity in its own right. She also executed the Agency Agreement in order to deceive the Department. It was effectively a sham arrangement and did not reflect how MSI Group operated in practice.

[96] All of these matters had the effect of keeping the true activities of MSI Group effectively hidden or disguised from the Department.

[97] Taking these factors into account I accept the Department's submission that an uplift of around 15 per cent is warranted for MSI Group as well. This means the overall starting point is increased to $4.485 million.

Mitigating factors

[98] There are no mitigating factors so far as these defendants are concerned that reduce the culpability of their conduct.

Totality

[99] It is now necessary to consider whether the pecuniary penalties produced by the above analysis are out of all proportion to the overall gravity of the breaches.

[100] I have already undertaken this exercise to some extent because I have taken into account the fact that some of the breaches overlap. Given the nature of the breaches, their duration and the other aggravating features I have identified I do not consider any further reduction is required to reflect totality principles.

[101] My conclusion is reinforced by the fact that the overall penalties I have selected are broadly in line with those imposed in *Ping An.* Like the present, that case involved serious and systemic breaches of numerous requirements of the Act over a prolonged period. It was also notable for the lack of co-operation and obstructive conduct shown by the defendant. The total penalty imposed in *Ping An* was $5.29 million.

Injunctive relief

[102] The Department seeks injunctions restraining both OTT and MSI from carrying out any financial activities that would cause either of them to be deemed to be a financial institution as defined in s 5 of the Act.

[103] Section 87 of the Act provides the Court with a discretion, on the Department's application, to grant an injunction "restraining a person from engaging in conduct that constitutes or would constitute a contravention of the Act". Section 88 then relevantly provides:

> **88 When High Court may grant restraining injunctions and interim injunctions**
>
> (1) The High Court may grant an injunction restraining a person from engaging in conduct of a particular kind if–
>
> (a) it is satisfied that the person has engaged in conduct of that kind; or
>
> (b) it appears to the court that, if an injunction is not granted, it is likely that the person will engage in conduct of that kind.
>
> …
>
> (3) Subsections (1)(a) and (2) apply whether or not it appears to the court that the person intends to engage again, or to continue to engage, in conduct of that kind.
>
> (4) Subsections (1)(b) and (2) apply–
>
> (a) whether or not the person has previously engaged in conduct of that kind; or
>
> (b) where there is an imminent danger of substantial damage to any other person if that person engaged in conduct of that kind.

[104] The Department seeks restraining injunctions against the individual defendants under s 87 of the Act. The purpose of such an injunction is to:[27]

> maintain and enhance New Zealand's international reputation in this area of financial activity, and … contribute to public confidence in New Zealand's financial sector. The threat of exclusion will also deter non-compliance by others.

---

[27] *Department of Internal Affairs v Ping An Finance (Group) New Zealand Ltd* above n 3, at [132].

[105] Given that both OTT and MSI have engaged in repeated, prolonged and serious contraventions of the Act, the first limb of s 88(1) is clearly made out. I am also satisfied that, if an injunction is not granted, OTT is likely to continue to contravene the Act.

[106] MSI Group had been struck off the Companies Register. It was reinstated on the Department's application solely for the purposes of this proceeding. I consider it unlikely that MSI will resume trading, or that there is any practical purpose of issuing injunctive relief against it.

Result

[107] I make an order under s 90(1) of the Act requiring OTT to pay to the Crown a pecuniary penalty in the sum of $3.1 million.

[108] I make an order under s 90(1) of the Act requiring MSI Group to pay to the Crown a pecuniary penalty in the sum of $4.485 million.

[109] I make a further order under s 87(1) of the Act restraining OTT, until further order of the Court, from carrying out any financial activities that would cause it to be deemed to be a financial institution as defined in s 5 of the Act.

Costs

[110] The Department is entitled to a joint and several award of costs on a category 2B basis together with disbursements as fixed by the Registrar against both OTT and MSI Group.

Lang J