

# FEDERAL COURT OF AUSTRALIA

## Australian Securities and Investments Commission v Macquarie Bank Limited [2024] FCA 416

File number(s): NSD 241 of 2022

Judgment of: **WIGNEY J**

Date of judgment: 19 April 2024

Date of publication: 29 April 2024

Catchwords: **CORPORATIONS** – provision of financial services – regulatory proceedings – where defendant holds an Australian financial services licence – whether financial services provider ensured that the financial services covered by the licence were provided “efficiently, honestly and fairly” – lack of adequate systems to prevent or detect fraudulent transactions by third parties in respect of client cash management accounts – admitted contravention of s 912A of the *Corporations Act 2001* (Cth) – declaration of contravention – agreed penalty – consideration of whether agreed penalty appropriate

Legislation: *Banking Act 1959* (Cth)  
*Corporations Act 2001* (Cth) ss 601FC(1)(b), 601FC(5), 761A, 764A(1)(i), 776A(1), 776C, 912A(1)(a), 912A(5A), 1317E(3), 1317G, 1657  
*Federal Court of Australia Act 1976* (Cth) s 21  
*Treasury Laws Amendment (Strengthening Corporate and Financial Sector Penalties) Act 2019* (Cth)

Cases cited: *Australian Building and Construction Commissioner v Pattinson* (2022) 274 CLR 450; [2022] HCA 13  
*Australian Competition and Consumer Commission v Construction, Forestry, Mining and Energy Union* (2007) ATPR 42-140; [2006] FCA 1730  
*Australian Competition and Consumer Commission v MSY Technology Pty Ltd* (2012) 201 FCR 378; [2012] FCAFC 56  
*Australian Securities and Investments Commission v Avestra Asset Management Ltd (in liq)* (2017) 348 ALR 525; [2017] FCA 497  
*Australian Securities and Investments Commission v Camelot Derivatives Pty Ltd (in liq)* (2012) 88 ACSR 206;

[2012] FCA 414 *Australian Securities and Investments Commission v Cassimatis (No 8)* (2016) 336 ALR 209; [2016] FCA 1023

*Australian Securities and Investments Commission v Commonwealth Bank of Australia* [2022] FCA 1422

*Australian Securities and Investments Commission v Mercer Financial Advice (Australia) Pty Ltd* [2023] FCA 1453

*Australian Securities and Investments Commission v National Australia Bank Limited* (2022) 164 ACSR 358; [2022] FCA 1324

*Australian Securities and Investments Commission v RI Advice Group Pty Ltd* (2022) 160 ACSR 204; [2022] FCA 496

*Australian Securities and Investments Commission v Rich* (2004) ACSR 500; [2004] NSWSC 836

*Australian Securities and Investments Commission v Westpac Banking Corporation (Omnibus)* (2022) 407 ALR 1; [2022] FCA 515

*Australian Securities and Investments Commission v Westpac Securities Administration Ltd* (2019) 373 ALR 455; [2019] FCAFC 187

*Commonwealth v Director, Fair Work Building Industry Inspectorate* (2015) 258 CLR 482; [2015] HCA 46

*Forster v Jododex Australia Pty Ltd* (1972) 127 CLR 421; [1972] HCA 61

*Hili v The Queen* (2010) 242 CLR 520; [2010] HCA 45

*McDonald v Australian Building and Construction Commissioner* (2011) 202 IR 467; [2011] FCAFC 29

*Rural Press Limited v Australian Competition and Consumer Commission* (2003) 216 CLR 53; [2003] HCA 75

*Volkswagen Aktiengesellschaft v Australian Competition and Consumer Commission* (2021) 284 FCR 24; [2021] FCAFC 49

Division: General Division

Registry: New South Wales

National Practice Area: Commercial and Corporations

Sub-area: Commercial Contracts, Banking, Finance and Insurance

Number of paragraphs: 94

Date of hearing: 19 April 2024

Counsel for the Plaintiff: Mr R Hollo SC with Mr D Luxton and Ms S Patterson

Solicitor for the Plaintiff: ASIC (Vic)

Counsel for the Defendant: Mr D Thomas SC with Ms L Coleman and Mr S Speirs

Solicitor for the Defendant: Allens

# ORDERS

NSD 241 of 2022

**BETWEEN:**                    **AUSTRALIAN SECURITIES AND INVESTMENTS  
COMMISSION**  
Plaintiff

**AND:**                         **MACQUARIE BANK LIMITED ACN 008 583 542**  
Defendant

**ORDER MADE BY:**   **WIGNEY J**

**DATE OF ORDER:**   **19 APRIL 2024**

## **THE COURT DECLARES THAT:**

1. Macquarie Bank Limited (**Macquarie**) contravened s 912A(1)(a) of the *Corporations Act 2001* (Cth) between 1 May 2016 and 12 March 2019, by failing to do all things necessary to ensure that the financial services covered by its financial services licence were provided efficiently, honestly and fairly, as a result of Macquarie not implementing effective controls to prevent or detect transactions conducted by third parties through Macquarie’s bulk transacting system that were outside the scope of the authority conferred on them that only permitted them to withdraw their fees from their clients’ Cash Management Accounts, such as the fraudulent transactions made by Mr Ross Hopkins.
2. Macquarie contravened s 912A(1)(a) and (5A) of the *Corporations Act 2001* (Cth) between 13 March 2019 and 15 January 2020, by failing to do all things necessary to ensure that the financial services covered by the financial services licence were provided efficiently, honestly and fairly, as a result of Macquarie not implementing effective controls to prevent or detect transactions conducted by third parties through Macquarie’s bulk transacting system that were outside the scope of the authority conferred on them that only permitted them to withdraw their fees from their clients’ Cash Management Accounts, such as the fraudulent transactions made by Mr Ross Hopkins.

## **THE COURT ORDERS THAT:**

1. Pursuant to s 1317G of the *Corporations Act 2001* (Cth), Macquarie pay to the Commonwealth of Australia within 28 days a pecuniary penalty in the amount of \$10,000,000.00 in respect of Macquarie's contravention s 912A(1)(a) and (5A) of the *Corporations Act* referred to in declaration 2 above.
2. Macquarie pay the plaintiff's costs of the proceeding as agreed or assessed within 28 days of such agreement or assessment.
3. The proceeding otherwise be dismissed.

Note: Entry of orders is dealt with in Rule 39.32 of the *Federal Court Rules 2011*.

## REASONS FOR JUDGMENT

*(Revised from transcript)*

### WIGNEY J:

1 **Macquarie** Bank Limited is a large and well-known financial institution that, among other things, holds a financial services licence and provides financial services to its many customers. The Australian Securities and Investments Commission (**ASIC**) commenced this proceeding against Macquarie alleging that it failed to do all things necessary to ensure that certain specified financial services covered by its financial services licence were provided efficiently, honestly, and fairly, and thereby contravened s 912A(1)(a) of the *Corporations Act 2001* (Cth). ASIC claimed, in short summary, that between 1 May 2016 and 15 January 2020, Macquarie failed to implement effective controls to prevent or detect fraudulent withdrawals by third parties from cash management accounts held by some of its clients. The account holders had given certain financial intermediaries, including financial advisers, stockbrokers, and accountants, limited authority to withdraw their fees from their cash management accounts via a bulk transacting system provided by Macquarie, but the absence of any effective controls in respect of that system permitted the intermediaries to conduct fraudulent withdrawals which were outside the scope of their authority. ASIC sought declarations of contravention by Macquarie and an order that Macquarie pay a pecuniary penalty in respect of its contravention.

2 While Macquarie initially defended the proceeding and opposed the declarations and orders sought by ASIC, it now admits that it contravened s 912A(1)(a) of the Corporations Act. It also consents to both the making of the declarations of contravention sought by ASIC and the making of an order that it pay the Commonwealth a pecuniary penalty in the amount of \$10,000,000.

3 While Macquarie consents to the making of those declarations and orders, it is nevertheless necessary for the Court to consider and determine whether the declarations and orders are appropriate and should be made.

### STATUTORY CONTEXT

4 The following references to provisions of the Corporations Act are to the text of those provisions at the time or times relevant to Macquarie's contravening conduct.

5 Section 912A(1)(a) of the Corporations Act provides:

- (1) A financial services licensee must:
- (a) do all things necessary to ensure that the financial services covered by the licence are provided efficiently, honestly and fairly ...

6 A person provides ‘financial services’ if they (relevantly) deal in a financial product: ss 766A(1) and 766C of the Corporations Act.

7 Section 912A(1)(a) was amended by the *Treasury Laws Amendment (Strengthening Corporate and Financial Sector Penalties) Act 2019* (Cth) (the **Amending Act**). Schedule 1, item 76 of the Amending Act inserted s 912A(5A), which had the effect of rendering s 912A(1)(a) a civil penalty provision.

8 Section 912A(5A) provides as follows:

- (5A) A person contravenes this subsection if the person contravenes paragraph (1)(a), (aa), (ca), (d), (e), (f), (g), (h) or (j).

Note: This subsection is a civil penalty provision (see section 1317E).

9 The Amending Act also inserted s 1657 of the Corporations Act which provides:

Subject to this Part, the amendments made by Schedule 1 to the [A]mending Act apply in relation to the contravention of a civil penalty provision if the conduct constituting the contravention of the provision occurs wholly on or after the commencement day.

10 The commencement day of Schedule 1 of the Amending Act, which inserted s 912A(5A), was 13 March 2019. As will be seen, that date is significant. It explains why ASIC has sought separate declarations concerning Macquarie’s conduct prior to 13 March 2019 and after that date. It is also important to note that the pecuniary penalty sought by ASIC only relates to Macquarie’s conduct after 13 March 2019.

11 There is no dispute that Macquarie was a financial services licensee. It was a financial services licensee because it held an Australian financial services license: see the definition of financial services licensee in s 761A of the Corporations Act.

12 There is also no dispute Macquarie’s conduct which is the subject of this proceeding occurred in the context of it providing financial services covered by that licence. That is because the relevant cash management accounts that Macquarie offered or provided to its customers were financial products within the meaning of s 764A(1)(i) of the Corporations Act, and by dealing with those accounts (see s 766C(1) of the Corporations Act), Macquarie provided financial services within the meaning of ss 766A(1)(b) of the Corporations Act. As there was no dispute

about those matters, it is unnecessary to set out the somewhat labyrinthine provisions of the Corporations Act that deal with them.

13 Subsection 1317E(1) provides that if a Court is satisfied that a person has contravened a civil penalty provision, it must make a declaration of contravention. Subsection 1317E(3) (in the form it was in during the relevant period) identifies provisions in the Corporations Act which are civil penalty provisions. Subsection 912A(5A) is identified as a civil penalty provision.

14 Subsection 1317G(1) of the Corporations Act provides that if the Court has made a declaration of contravention of a civil penalty provision pursuant to s 1317E, it ‘may’ order the person to pay to the Commonwealth a pecuniary penalty. The pecuniary penalty must not exceed the pecuniary penalty applicable to the contravention: s 1317G(2).

15 Subsection s 1317G(4) of the Corporations Act provides that the pecuniary penalty applicable to the contravention of a civil penalty provision by a body corporate is the greatest of:

- (a) 50,000 penalty units;
- (b) if the Court can determine the benefit derived and detriment avoided because of the contravention – that amount multiplied by 3; and
- (c) either:
  - (i) 10% of the annual turnover of the body corporate for the 12-month period ending at the end of the month in which the body corporate contravened, or began to contravene, the civil penalty provision; or
  - (ii) if the amount worked out under subparagraph (i) is greater than the amount equal to 2.5 million penalty units – 2.5 million penalty units.

16 It is common ground that the pecuniary penalty applicable to the contravention by Macquarie is the penalty calculated pursuant to s 1317G(4)(c)(ii) because the figure representing 10% of the annual turnover of Macquarie during the relevant 12-month period is greater than \$525,000,000, being 2.5 million penalty units (at the time of the contravention in question the value of a penalty unit was \$210), and there was no suggestion that the Court could determine any benefit derived by reason of the contravention in accordance with s 1317G(4)(b).

17 The maximum penalty for the relevant contravention by Macquarie is accordingly \$525,000,000.



18 Section 1317G(6) of the Corporations Act provides that, in determining the pecuniary penalty, the Court must take into account “all relevant matters”, including: the nature and extent of the contravention; the nature and extent of any loss or damage suffered because of the contravention; the circumstances in which the contravention took place; and whether the person has previously been found by a court to have engaged in any similar conduct. The relevant matters identified in s 1317G(6) are plainly not exhaustive.

### MACQUARIE’S CONTRAVENING CONDUCT

19 The parties jointly relied upon a Statement of Agreed Facts and Admissions. A copy of that document (not including Confidential Annexure A, and redacted in accordance with a suppression order made by the Court) is attached to this judgment at Annexure A. There is no basis for the Court to believe or conclude that the agreed facts are inaccurate or incomplete in any material respect. Indeed, they identify the contravening conduct in very clear and painstaking detail.

20 It is unnecessary to rehearse the facts in any detail in this judgment. Following is a short summary of the salient facts. The facts relate to the period 1 May 2016 to 15 January 2020 unless otherwise indicated. That period is generally referred to as the **relevant period**.

21 Macquarie was an authorised deposit-taking institution for the purposes of the *Banking Act 1959* (Cth) and held an Australian Financial Services Licence (**AFSL**).

22 Macquarie offered its customers a deposit account product called a Cash Management Account (**CMA**).

23 CMAs were deposit-taking facilities made available by Macquarie in the course of its banking business. As such, they were ‘financial product[s]’ within the meaning of s 764A(1)(i) of the Corporations Act. In issuing CMAs, Macquarie dealt with financial products and provided financial services within the meaning of ss 766A(1)(b) and 766C(1) of the Corporations Act. Those financial services were covered by the terms of Macquarie’s AFSL.

24 CMAs allowed for various transfers to be made to or from the account, including: the transfer of funds to term deposit accounts; the transfer of funds to purchase shares; the transfer of funds to invest in managed funds; the transfer of funds for the payment of fees to third party intermediaries; the receipt of investment returns such as dividends and interest. Macquarie’s CMA customers could grant third party financial intermediaries, such as financial advisers, authority to withdraw funds from their CMAs. There were different levels of authorities,

ranging from a general authority which effectively permitted any transaction, to a limited authority which only permitted the payment of a third party's fees.

25 Macquarie made available a 'bulk transacting' system or facility for effecting transactions on CMAs. That facility or system enabled third parties who had been granted an authority by account holders to, among other things, effect multiple withdrawals from multiple CMAs at once. To access that facility, a third party was required to register with Macquarie, distribute Macquarie products, and obtain access to an online facility operated by Macquarie. The third party was also required to complete and upload a template or data file. One such template was a fee payments template, which was the applicable template where the transaction type was the payment of fees and the CMA holder had granted a fee authority.

26 Bulk transactions involving the payment of fees using the bulk transaction system or facility involved inherent risks for customers, particularly risks associated with fraudulent or otherwise unauthorised transactions by third party intermediaries who had been granted authorities by the account holder.

27 Macquarie put in place some systems or controls to mitigate the risk of fraudulent transactions by third parties acting beyond the scope of their fee authorities. For example, by early 2014, bulk transactions involving fees generated an email alert if they contained one or more transactions for an amount which exceeded a certain specified amount (the **alerts**). There was, however, no written practice or procedure in place to review or monitor the alerts. As a result, the alerts had little or no effect in mitigating the risk of fraudulent transactions.

28 Between about mid-2012 and mid-2016, certain Macquarie employees became aware that some financial intermediaries had misused their fees authorities by conducting bulk transactions ostensibly in respect of fees, but for purposes other than the payment of fees. A number of those instances of misuse involved a financial adviser named Mr Ross **Hopkins**, though he was not the only third party involved in such wrongdoing. Some steps were taken to deal with that issue. Those steps, however, were obviously inadequate and ineffective.

29 From about mid-2016, various Macquarie employees prepared papers and presentations, and undertook reviews, in which they identified the clear risk that bulk transacting, including bulk transacting involving fees, could be used by third parties to effect fraudulent or unauthorised transactions on CMAs held by Macquarie clients. It is unnecessary to spell out in detail the content of those papers, presentations, and reviews, or what they uncovered and recommended

could or should be done. The details are contained in the Statement of Agreed Facts and Admissions. Suffice it to say that, despite what was uncovered or discovered during those processes concerning fraudulent transactions and the ongoing risks inherent in bulk transacting without further controls, Macquarie failed to implement effective controls to prevent or detect bulk transactions involving fees that were outside the scope of the limited fee authority conferred on third parties until January 2020.

30 The upshot of Macquarie's failures in that regard was that it did not detect 167 fraudulent transactions, totalling almost \$3,000,000 that were effected by Mr Hopkins in the period October 2016 to October 2019 utilising Macquarie's bulk transaction system or facility in respect of 14 CMAs held by 13 of his clients. Those transactions included 97 transactions that gave rise to alerts, though as explained earlier, those alerts were not systematically reviewed.

31 Macquarie's failures in that regard were effectively remedied in January 2020 when it implemented a real-time alert system which alerted CMA holders of transactions initiated by persons to whom they had granted authorities, including fee authorities. In May 2020, Macquarie also implemented a fraud monitoring program for bulk transacting. A review conducted in late 2020 or early 2021 did not identify any further instances of fraudulent transactions involving bulk transactions concerning fees.

32 Some additional facts should be highlighted to provide appropriate context. As at August 2017, over half a million customers held a Macquarie CMA and over \$26 billion was under management or on deposit in respect of CMA products. CMA customers mostly had external financial advisers and were long term customers of Macquarie. The monthly volume of transactions using the fee payments template during the relevant period ranged from about \$174 million to about \$477 million.

33 Macquarie admitted that between 1 May 2016 and 12 March 2019, it failed to do all things necessary to ensure that the financial services covered by its financial services licence were provided efficiently, honestly, and fairly, as a result of it not implementing effective controls to prevent or detect transactions conducted by third parties through its bulk transacting system that were outside the scope of the authority conferred on them that only permitted them to withdraw their fees from their clients' CMAs, such as the fraudulent transactions made by Mr Hopkins.

34 Macquarie similarly admitted that between 13 March 2019 and 15 January 2020, it failed to do all things necessary to ensure that the financial services covered by its financial services licence were provided efficiently, honestly, and fairly, as a result of it not implementing effective controls to prevent or detect transactions conducted by third parties through its bulk transacting system that were outside the scope of the authority conferred on them that only permitted them to withdraw their fees from their clients' CMAs, such as the fraudulent transactions made by Mr Hopkins.

35 The reason for the separate admissions by Macquarie and ASIC's application for separate declarations in respect of those two periods was explained earlier.

#### **ADDITIONAL FACTS RELEVANT TO PENALTY**

36 The Statement of Agreed Facts and Admissions also includes the following facts which were said to be relevant to the assessment of the appropriate pecuniary penalty.

37 Macquarie was, and is, a very large and profitable company. For the 2016 to 2020 financial years, Macquarie's net operating income ranged between about \$5 billion and about \$6.2 billion, its net profit after tax ranged between about \$1 billion and \$1.3 billion, its total assets ranged between about \$164 billion and \$226 billion and its net assets ranged between \$11.2 billion and \$14.2 billion.

38 Macquarie was, and is, a subsidiary of **Macquarie Group** Limited, a public company listed on the Australian Stock Exchange. For the 2016 to 2020 financial years, Macquarie Group's market capitalisation ranged between \$22.5 billion and \$44 billion.

39 As at 31 March 2019, Macquarie and its related bodies corporate had an 'annual turnover' within the meaning of the Corporations Act of more than \$5,250,000,000. That fact is particularly relevant as it provides the basis for the calculation of the maximum pecuniary penalty for Macquarie's contravention of s 912A(1)(a) referable to the period from 13 March 2019 to 15 January 2020.

40 The Statement of Agreed Facts and Admissions contains details of the seniority and reporting lines of the Macquarie employees who were aware that Macquarie's monitoring and control of bulk transacting concerning fees during the relevant period was deficient. It suffices for present purposes to note that those employees were quite senior. They reported up two or three reporting lines to the chief executive officer of Macquarie Group. There was, however, no

evidence to suggest that Macquarie’s directors at the time were aware of the facts giving rise to the contravention.

41 Macquarie has not previously been found by any court to have contravened s 912A of the Corporations Act, and no court has previously made any declaration that Macquarie has contravened a civil penalty provision under the Corporations Act or made any order that Macquarie pay a penalty in respect of such a contravention.

42 On 23 August 2016, the Supreme Court of New South Wales found that **Macquarie Investment Management** Limited had contravened ss 601FC(1)(b) and 601FC(5) of the Corporations Act. At that time, Macquarie Investment Management was a subsidiary of both Macquarie Group and Macquarie.

43 ASIC commenced its investigation into Macquarie regarding its CMAs and the conduct of Mr Hopkins on about 22 September 2020. The investigation concluded when ASIC commenced this proceeding in April 2022. During the investigation, Macquarie engaged openly and transparently with ASIC, engaged in voluntary meetings with ASIC, and provided information about the availability and structure of data that could be provided to ASIC in respect of the investigation.

44 Since the commencement of this proceeding, Macquarie: agreed to a statement of agreed facts for use in the proceeding if it proceeded to a contested hearing; responded promptly to requests by ASIC for clarification and the production of documents in connection to this proceeding; and attended a mediation and ultimately admitted liability in this proceeding. Macquarie also participated in the process resulting in the Agreed Statement of Facts and Admissions and joint written submissions.

### **RELEVANT PRINCIPLES**

45 The principles which are relevant to determine the issues before the Court were not in issue and need only be addressed in short terms.

### **Section 912A(1)(a) of the Corporations Act**

46 The standard created by the words “efficiently, honestly and fairly” in s 912A(1)(a) of the Corporations Act has been considered in a number of cases, including: *Australian Securities and Investments Commission v Camelot Derivatives Pty Ltd (in liq)* (2012) 88 ACSR 206; [2012] FCA 414 at [69]-[70]; *Australian Securities and Investments Commission v Cassimatis*

(No 8) (2016) 336 ALR 209; [2016] FCA 1023 at [674]; *Australian Securities and Investments Commission v Avestra Asset Management Ltd (in liq)* (2017) 348 ALR 525; [2017] FCA 497 at [191]; *Australian Securities and Investments Commission v Westpac Securities Administration Ltd* (2019) 373 ALR 455; [2019] FCAFC 187; *Australian Securities and Investments Commission v National Australia Bank Limited* (2022) 164 ACSR 358; [2022] FCA 1324; and *Australian Securities and Investments Commission v Commonwealth Bank of Australia* [2022] FCA 1422.

47 Different views have been expressed as to whether “efficiently, honestly and fairly” comprises a single compendious standard or imposes three concurrent obligations. It is unnecessary to decide that issue in this case. Macquarie has admitted that it failed to meet the standard in any event. It is also somewhat difficult to see how or why it would make any practical difference if there was a single compendious standard, as opposed to three concurrent standards or obligations. It is also doubtful that there is any real utility in exploring in the abstract the meaning of what are otherwise ordinary words, the meaning of which is generally well understood. Nevertheless, the following useful principles emerge from some of the authorities.

48 First, the standard of honesty is to be considered having regard to commercial norms and morality, as opposed to the broader societal norms that generally inform the meaning of the standard of honesty in the criminal law. A licensee may fail to meet the standard of honesty even though its conduct could not be said to be criminally dishonest.

49 Second, a licensee may breach or fail to comply with the obligation created by s 912A(1)(a) even if it has not breached any separate legal duty or obligation under the Corporations Act or otherwise.

50 Third, the standard, or standards, imposed by s 912A(1)(a) do not require absolute perfection by the licensee in providing financial services.

51 Fourth, the use of the word “ensure” tends to indicate that compliance with the obligation created by s 912A(1)(a) involves or requires a degree of forward looking and may require the licensee to take steps to prevent future lapses or failures.

### **Declarations of contraventions**

52 As noted earlier, s 1317E(1) provides that if a Court is satisfied that a person has contravened a civil penalty provision, it *must* make a declaration of contravention. It is nevertheless useful to briefly consider the general principles that apply in respect of the making of declarations.

53 The Court has a wide discretionary power to make declarations under s 21 of the *Federal Court of Australia Act 1976* (Cth).

54 Before making a declaration, even by consent, the Court must be satisfied that: first, the proceeding involves a real controversy, as opposed to hypothetical or theoretical question; second, that the applicant has a real interest in raising the controversy or question; and third that there is a proper contradictor: *Forster v Jododex Australia Pty Ltd* (1972) 127 CLR 421 at 437-438; [1972] HCA 61.

55 The fact that a respondent who has a real interest in opposing the declaration nevertheless consents to the making of the declaration does not mean that there is no contradictor: *Australian Competition and Consumer Commission v MSY Technology Pty Ltd* (2012) 201 FCR 378; [2012] FCAFC 56 at [30]-[33].

56 Where the declaration concerns a contravention of a civil penalty provision, the Court must be satisfied that the respondent contravened that provision, even if the respondent consents to the making of the declaration. The material that provides the basis for the Court's satisfaction can be a statement of agreed facts and admissions: *Australian Securities and Investments Commission v Rich* (2004) ACSR 500; [2004] NSWSC 836 at [15].

57 Declarations relating to contraventions of legislative provisions are likely to be appropriate where they serve to record the Court's disapproval of the contravening conduct, vindicate a regulator's claim that the respondent contravened the provisions, assist a regulator to carry out its duties, and deter other persons from contravening the provisions: *Australian Competition and Consumer Commission v Construction, Forestry, Mining and Energy Union* (2007) ATPR 42-140; [2006] FCA 1730 at [6] (and the cases cited therein).

58 The Court must be satisfied that a proposed declaration of contravention identifies the conduct that constituted the contravention or the gist of the findings that amounted to the contravention: *Rural Press Limited v Australian Competition and Consumer Commission* (2003) 216 CLR 53; [2003] HCA 75 at [89].

### **Agreed penalties**

59 The principles that the Court must apply in considering whether to impose an agreed pecuniary penalty jointly proposed by the parties were explained in *Commonwealth v Director, Fair Work Building Industry Inspectorate* (2015) 258 CLR 482; [2015] HCA 46 (*Agreed Penalties Case*).

60 In short summary, the Court must consider and determine whether the agreed penalty is within the range of possible penalties that the Court could reasonably impose in all the circumstances. If the agreed penalty is within that range, the public policy of promoting the predictability of outcomes in civil penalty proceedings makes it highly desirable for the Court to accept the parties' joint proposal and impose the agreed penalty. The court is nevertheless not bound by the parties' agreement in respect of the size of the penalty.

### **Pecuniary penalties generally**

61 In considering and determining whether the agreed penalty falls within the range of appropriate penalties in the circumstances, it is necessary to have regard to the applicable principles concerning the fixing of pecuniary penalties. Those principles are also settled. They were recently considered in *Australian Building and Construction Commissioner v Pattinson* (2022) 274 CLR 450; [2022] HCA 13.

62 In short summary, the purpose of imposing a civil penalty is to promote the public interest in compliance with the relevant Act by the deterrence of further contraventions of a like kind. The Court must, in effect, attempt to put a price on contravention that is sufficiently high to deter repetition by the contravener and by others who might be tempted to contravene. The penalty must not be one which would be regarded by the contravener or others as an acceptable cost of doing business. The penalty must not, however, be greater than is necessary to achieve the object of deterrence. An appropriate penalty is said to be one that strikes an appropriate balance between oppressive severity and the need for deterrence in the particular case.

63 In determining the size of the penalty which would serve the objective of deterrence, the Court must have regard to both the circumstances of the contravener and the circumstances of the contravention.

64 Without intending to be exhaustive, the factors concerning the circumstances of the contravener which are generally relevant when determining the size of the penalty which would serve the objective of deterrence, where the contravener is a corporation, include: the size and financial position of the corporation; whether the corporation has a corporate culture conducive to compliance with the relevant Act; whether the contravener has engaged in similar conduct in the past; and whether the contravener has demonstrated contrition and co-operated with the relevant authorities.



65 Likewise, without intending to be exhaustive, the factors concerning the circumstances of the contravention which are generally relevant to determining the size of the penalty which would serve the objective of deterrence include: whether the contravening conduct was systematic, deliberate or covert; the period over which the contravening conduct occurred; whether the contravention arose out of the conduct of senior management; whether the contravener profited from the contravention and if so the extent of that profit; and whether the contravention caused any loss or injury.

66 It should be emphasised that both the factors relating to the circumstances of the contravener, and those relating to the circumstances of the contravention, are only relevant to the extent that they bear on the question of the size of the penalty that is necessary to achieve the objective of deterrence. The purpose of imposing a pecuniary penalty does not include retribution or punishment. The pecuniary penalty need not be proportionate to the nature and circumstances of the contravention, at least in the sense that the principle of proportionality is understood in the criminal law.

67 The maximum penalty is also a relevant consideration in determining the size of the penalty, though it does not constrain the exercise of the discretion beyond requiring some reasonable relationship between the theoretical maximum and the final penalty imposed. The maximum penalty would generally only be appropriate in the case of a contravention which warranted the strongest deterrence.

#### **DECLARATION OF CONTRAVENTION BY MACQUARIE**

68 As has already been noted, Macquarie admitted that its conduct between 1 May 2016 and 15 January 2020 in failing to implement effective controls to prevent or detect conduct by third parties through its bulk transacting system that were outside the scope of the authority conferred on them in respect of fees contravened s 912A(1)(a) of the Corporations Act. I am also satisfied, having regard to the principles referred to earlier, that the agreed facts establish that Macquarie contravened s 912A(1)(a) of the Corporations Act during the relevant period.

69 While there was, in effect, a single contravention arising from the conduct throughout the relevant period, as explained earlier, ASIC sought two declarations because the amendments to the Corporations Act only made s 912A(1)(a) a civil penalty provision on, and from, 13 March 2019.

70 In light of Macquarie's admissions, it is unnecessary to provide detailed reasons for finding that the agreed facts establish Macquarie's contravention. It suffices to refer to the following key points that emerge from the agreed facts.

71 First, by allowing and facilitating its CMA customers to authorise third parties to deduct their fees from their CMA, and then enabling the third parties to utilise the bulk transacting system or facility, Macquarie effectively exposed their customers to the risk that the third parties might conduct fraudulent transactions outside the terms of their authorities.

72 Second, Macquarie was no doubt aware of that risk during the relevant period. Specifically, it was aware that third parties who had been granted authorities in respect of their fees might misuse those authorities when using the bulk transacting system or facility. Indeed, it was aware that third party intermediaries, including Mr Hopkins, had so misused their authorities.

73 Third, in those circumstances, in order to ensure that it provided its financial services efficiently, honestly, and fairly, it was incumbent on Macquarie to have, or to put in place, effective controls to prevent or detect transactions conducted by third parties which were outside the scope of their limited authorities. While Macquarie put in place some controls, such as the alerts, those controls were plainly deficient or inadequate. In the case of the alerts, they were not systematically reviewed.

74 Fourth, there were no effective or insurmountable barriers which prevented or excused Macquarie from putting effective controls in place. Nor was Macquarie's conduct adequately explained or its failures absolved by factors such as the high volume of bulk transactions.

75 As for the making of the declarations sought by ASIC, I am satisfied that the proceeding involves a real controversy, that ASIC had, and has, a real interest in raising the controversy, and that Macquarie was an appropriate and effective contradictor in all the circumstances. I am also satisfied that the declarations are appropriate as they serve to record the Court's disapproval of Macquarie's contravening conduct, vindicate ASIC's claim that Macquarie contravened the provisions, and will operate to deter other persons from contravening s 912A(1)(a) in a similar or comparable way. Needless to say, I am also satisfied that Macquarie contravened s 912A(1)(a) in the manner referred to in the declarations.

76 As for the form of the declarations, I am satisfied that the agreed terms of the declarations are appropriate. They adequately identify the conduct that constituted the contravention.

77 In all the circumstances, it is appropriate for the Court to make the declarations sought by ASIC and agreed to by Macquarie.

### **THE PECUNIARY PENALTY TO BE PAID BY MACQUARIE**

78 I am persuaded that the agreed penalty of \$10,000,000 is *an* appropriate penalty in all the circumstances, in the sense that I consider that is within the range of possible penalties that the Court could reasonably impose in all the circumstances of the case. I do not suggest that I would necessarily have imposed that precise penalty had I not been confronted with the parties' agreement and joint submissions, though that is essentially beside the point. I am nevertheless satisfied that it is appropriate to make the agreed penalty order for the purposes identified in the *Agreed Penalties Case*.

79 The main factors relevant to the assessment of an appropriate penalty in this case may be summarised as follows.

80 First, there could be little doubt that the contravention in respect of which the pecuniary penalty is to be imposed was a serious contravention of s 912A(1)(a) of the Corporations Act. It occurred over a 10-month period, though it must, to an extent, be considered in the context of the earlier contravening conduct, being the conduct which occurred before 13 March 2019. The contravention involved quite senior employees of Macquarie, being those employees who had become aware of the inadequacies and deficiencies of the controls that Macquarie had in place and who, it may be inferred, failed to take, or cause others to take, the necessary and appropriate steps to ensure that the inadequacies and deficiencies were appropriately addressed. As a result of the contravening conduct, Macquarie's CMA clients who had granted fee authorities to third parties were at risk of fraudulent activity on their accounts. The contravening conduct in fact resulted in losses to CMA clients as a result of Mr Hopkins's conduct totalling at least \$2,938,750, \$701,500 of which occurred on or after 13 March 2019.

81 Second, there are nevertheless some features of the contravening conduct that moderate the seriousness of the contraventions. The contravening conduct was not in any relevant sense deliberate or even reckless. Rather, the contravention was the product of a degree of neglect, laxity or inaction on the part of certain employees of Macquarie. The deficiencies and inadequacy of the existing controls in respect of bulk transacting was known to, and recognised by, Macquarie, as was the risk to CMA clients who had granted fee authorities, but not enough was done to address the inadequacies and deficiencies, or eliminate the risks to CMA clients. Macquarie received no direct financial benefit from the contravening conduct, though it could

perhaps be said that it avoided, or at least deferred, the cost that was most likely involved in remedying the inadequate controls.

82 Third, the seriousness of the offending conduct does not itself necessarily compel or require the imposition of a very large penalty. As discussed earlier, the purpose for which a pecuniary penalty is imposed is to deter, not to punish. There is no retributive purpose in imposing a pecuniary penalty. Nor is it necessary for the penalty to be proportionate to the seriousness of the offence in the same way that, for example, a criminal sanction must “fit the crime”. The features of the contravening conduct that render it a serious contravention are only relevant in assessing the size of the penalty if they suggest that, in light of those features, a larger penalty is required to achieve the purpose of deterrence, both specific and general. In this case, despite the seriousness of the contravening conduct, the fact that the contravention was not deliberate or reckless, let alone contumelious, would tend to suggest that an especially large penalty is not required to achieve specific deterrence.

83 Fourth, there are some factors relating to Macquarie’s circumstances that also bear directly on the size of the penalty that is necessary to appropriately secure specific deterrence. Macquarie has not previously been found to have been involved in any contraventions of civil penalty provisions in the Corporations Act or been found to have engaged in any conduct similar to the contravening conduct involved in this matter. It is certainly not a recidivist or recalcitrant contravener. While there is no evidence of any clear or direct expression of contrition or remorse on Macquarie’s behalf, nevertheless some degree of contrition can be inferred from the fact that Macquarie ultimately admitted its contravention. It also cooperated, to an extent, with ASIC’s investigation and displayed a willingness to facilitate the course of justice by making admissions and joining in the Agreed Statement of Facts and Admissions and joint submissions.

84 Fifth, Macquarie is a very large and very profitable corporation. If, as has been said to be the case, the court must fix a penalty which puts a price on the contravention that is sufficiently high to deter repetition, the size and financial capacity of Macquarie would tend to suggest that anything other than a very large penalty would have little or no deterrent effect in respect of Macquarie itself. A penalty that might be seen as very being large and as having a significant deterrent effect by many corporations would be likely to be considered to be piffling to Macquarie having regard to its size and financial resources. That said, it would plainly be

wrong to impose a very large penalty on Macquarie in respect of this contravention simply because it is a large and profitable corporation.

85 Sixth, in fixing an appropriate penalty in the case of a contravention like the one the subject of this case, the Court must not lose sight of the importance of general deterrence. The reality is that many financial services licensees are, like Macquarie, large and profitable corporations. If the Court imposes penalties for contraventions of s 912A(1)(a) of the Corporations Act, or similar provisions, which are likely to be seen by financial services licensees generally as being modest or insignificant, they will have little effect in deterring others from engaging in similar conduct.

86 Seventh, while it is necessary to have some regard to the very large maximum penalty for Macquarie's contravention, the maximum penalty is only one of many relevant considerations. In this case, it is of quite limited relevance. A penalty approaching the maximum penalty in this case would only be appropriate if the circumstances of Macquarie's contravening conduct, and the circumstances pertaining to Macquarie itself, suggested that the strongest possible deterrence was warranted. I do not consider that the circumstances of this case are such that anything like the strongest possible deterrence is warranted.

87 Eighth, it is relevant, and of some significance, that ASIC has agreed that \$10,000,000 is an appropriate penalty in all the circumstances. As a specialist regulator, ASIC may be taken to have some insight and expertise in assessing the level of penalty that might appropriately secure deterrence, both specific and general, in the circumstances of the case: *Agreed Penalties Case* at [60]-[61]. That said, the joint submissions must be assessed on their merits, and the Court must be wary of the possibility that the agreed penalty may be the product of the regulator having been too pragmatic in reaching the settlement: *Agreed Penalties Case* at [61], [110]; *Volkswagen Aktiengesellschaft v Australian Competition and Consumer Commission* (2021) 284 FCR 24; [2021] FCAFC 49 at [129]. There is, however, nothing to suggest that ASIC took an overly pragmatic approach in this matter when it reached an agreement with Macquarie in respect of the size of the pecuniary penalty.

88 Ninth, the Court's attention has been drawn to the penalties that have been imposed in some other cases involving contraventions of s 912A(1)(a) of the Corporations Act, in particular: *Australian Securities and Investments Commission v Westpac Banking Corporation (Omnibus)* (2022) 407 ALR 1; [2022] FCA 515; *Australian Securities and Investments Commission v Mercer Financial Advice (Australia) Pty Ltd* [2023] FCA 1453; *Australian Securities and*

*Investments Commission v RI Advice Group Pty Ltd* (2022) 160 ACSR 204; [2022] FCA 496. The parties correctly conceded, however, that those cases are of limited assistance when it comes to the fixing of the appropriate penalty in this case. It is consistency in the application of the relevant legal principles that is important, not consistency in numerical outcome: *McDonald v Australian Building and Construction Commissioner* (2011) 202 IR 467; [2011] FCAFC 29 at [23]-[25], referring to *Hili v The Queen* (2010) 242 CLR 520; [2010] HCA 45 at [48]. Each case must be considered having regard to its own unique facts and circumstances. The outcome in other cases is of even less assistance where the penalties imposed in them were agreed penalties. That is because the most that could be said in those circumstances is that the penalties imposed by the Court were within the range of penalties that the Court could reasonably impose in the circumstances of those cases.

89 Nevertheless, nothing in the previous cases involving the imposition of penalties for contraventions of s 912A(1)(a) of the Corporations Act would suggest that the agreed penalty in this case is outside the range of penalties that the Court could reasonably impose.

90 In all the circumstances, I accept that a pecuniary penalty of \$10,000,000 is an appropriate penalty in the sense that it is likely to serve the objective of deterrence and cannot be said to be greater than is necessary to achieve that objective.

## **DISPOSITION**

91 The Court will make the declarations sought by ASIC and agreed by Macquarie in respect of Macquarie's contraventions of s 912A(1)(a) of the Corporations Act.

92 Macquarie will be ordered to pay a pecuniary penalty of \$10,000,000 in respect of its contravention of s 912A(1)(a) of the Corporations Act that occurred on and after 13 March 2019.

93 The parties also agreed that Macquarie should be ordered to pay ASIC's costs of the proceeding as agreed or assessed.

94 Finally, the parties applied for a suppression order in respect of a document annexed to the Agreed Statement of Facts and Admissions (Confidential Annexure A), as well as some parts of the Statement of Agreed Facts and Admissions that, like Confidential Annexure A, reveal the content of fraud monitoring rules that Macquarie put in place after the relevant period. I am satisfied that a suppression order should be made in respect of that document on the basis that it is necessary to prevent prejudice to the proper administration of justice. Plainly the

content of any fraud monitoring rules put in place by Macquarie should remain confidential, otherwise unscrupulous persons could endeavour to work out ways to circumvent those rules. The precise terms of the suppression order have not yet been settled. That order will accordingly be made at a later date.

I certify that the preceding ninety-four (94) numbered paragraphs are a true copy of the Reasons for Judgment of the Honourable Justice Wigney.

Associate:

A handwritten signature in black ink, appearing to be 'M. D. M.', written in a cursive style.

Dated: 29 April 2024

## **ANNEXURE A – STATEMENT OF AGREED FACTS AND ADMISSIONS**



**Statement of Agreed Facts and Admissions**

Federal Court of Australia

District Registry: New South Wales

Division: General

No. NSD 241 of 2022

**IN THE MATTER OF MACQUARIE BANK LIMITED ACN 008 583 542**

**AUSTRALIAN SECURITIES AND INVESTMENTS COMMISSION**

Plaintiff

and

**MACQUARIE BANK LIMITED ACN 008 583 542**

Defendant

**A. INTRODUCTION**

1. This Statement of Agreed Facts and Admissions (**SAFA**) is made for the purposes of s 191 of the *Evidence Act 1995* (Cth) jointly by the plaintiff, the Australian Securities and Investments Commission (**ASIC**), and the defendant, Macquarie Bank Limited (**Macquarie**).
2. The SAFA relates to a proceeding commenced by ASIC against Macquarie on 4 April 2022 (**Proceeding**). This SAFA is made jointly by ASIC and Macquarie in support of consent orders setting out the relief and other orders they agree to, which, if made, will resolve this Proceeding.
3. This document contains facts relevant to two contraventions of s 912A(1)(a) of the *Corporations Act 2001* (Cth) (**Corporations Act**) alleged by ASIC and admitted to by Macquarie for the purposes of the Proceeding. The facts agreed to, and the admissions made, are agreed to and made solely for the purposes of the Proceeding and do not constitute any admission outside of the Proceeding.

## B. THE PARTIES

### *ASIC*

4. At all material times, ASIC is and was a body corporate established under s 7 of the *Australian Securities Commission Act 1989* (Cth), continued by s 261 of the *Australian Securities and Investments Commission Act 2001* (Cth) (**ASIC Act**), and able to sue in its corporate name by reason of s 8 of the ASIC Act.

### *Macquarie*

5. Macquarie is and was, at all material times, an authorised deposit-taking institution (**ADI**) for the purposes of the *Banking Act 1959* (Cth).
6. Since 1 March 2004, Macquarie has been the holder of an Australian Financial Services Licence (**AFSL**) numbered 237502. Macquarie's AFSL authorised it to carry on a financial services business, including in respect of the provision of: financial product advice for deposit and payment products; dealing in a financial product by issuing, applying for, acquiring, varying or disposing of a financial product in respect of deposit and payment products; and dealing in a financial product by applying for, acquiring, varying or disposing of a financial product on behalf of another person in respect of deposit and payment products.

### *Interpretation*

7. In this SAFA:
  - (a) **CMA** means a Cash Management Account which is a product offered by Macquarie.
  - (b) **Fees Bulk Transacting** means the use of the processes and templates for making fee payments through the Bulk Transacting system as set out in this SOAF.
  - (c) **Fees Bulk Transactions** means the transactions effected through the use of Fees Bulk Transacting.
  - (d) **Financial Intermediary or FI** means a company, firm, sole trader or partnership that acts on a client's behalf in respect of their use of, or investments in, Macquarie products, such as a financial advisory, stockbroking or accounting firm or self-

managed super fund or wealth platform business administrator or mortgage broker.

- (e) **Relevant Period** means the period from 1 May 2016 to 15 January 2020;
- (f) **Penalty Period** means the period from 13 March 2019 to 15 January 2020;
- (g) **Representative** means:
  - (i) a corporate representative (including its appointed natural person representatives) appointed by a Financial Intermediary; or
  - (ii) a natural person (such as a financial advisor) who has been appointed by a Financial Intermediary,

to approve and upload transactions through the Bulk Transacting System or make payments through AIP.

- 8. Headings used in this SAFA are adopted for convenience only. ASIC and Macquarie do not admit any factual assertions contained in or implied by any heading used in this SAFA.

#### C. BACKGROUND

- 9. During the Relevant Period, the operations of Macquarie and Macquarie Group Limited (Macquarie's parent company) were organised into operating groups (**Operating Groups**). The Banking and Financial Services Group (**BFS Group**) was an Operating Group sitting within that organisational structure.
- 10. Primary responsibility for risk management within the BFS Group belonged to that Operating Group. That is, the BFS Group had ownership of risks that arose in, or because of, its operations. According to Macquarie's Risk Management Strategy, this required it to have systems, resources, management processes and operational controls in place for identifying, measuring, evaluating, monitoring, and controlling or mitigating material risks, in accordance with Macquarie's risk management framework. The risk owner formed the first line of defence (**Line 1**).
- 11. The Risk Management Group (**RMG**) was one of the four central service groups that provided services across all Operating Groups, including the BFS Group. RMG formed the second line of defence (**Line 2**) and provided independent and objective review and challenge,

oversight, monitoring and reporting of Macquarie's material risk. RMG was functionally independent from the first line of defence.

12. The BFS Group comprised Macquarie's retail banking and financial services businesses, and provided a range of personal banking, wealth management, and business banking products and services to retail clients, advisers, brokers and business clients. This included the offering of the 'Cash Management Account', described in paragraphs 24 to 28 below.

13. During the Relevant Period, the BFS Group was:

- (a) organised into three distinct channels (**Channels**) comprising:
  - (i) Personal Banking;
  - (ii) Wealth Management; and
  - (iii) Business Banking.
- (b) separated into service groups that provided the services across those Channels (**Divisions**).

14. During the Relevant Period until about May 2018, the Divisions of the BFS Group were:

- (a) People, Culture and Client Experience;
- (b) Corporate Development and Strategy;
- (c) Product and Projects;
- (d) Service Sales Centre and Operations, which included the Fees and Commissions team (prior to the Relevant Period, this team had been known as the Adviser and Online Services (**A&OS**) team);
- (e) BFS Central which was organised into subdivisions, including:
  - (i) Marketing;
  - (ii) Information Management;
  - (iii) Human Resources;

- (iv) Finance;
- (v) Credit & Risk;
- (vi) Technology;
- (vii) Corporate Communications and Investor Relations; and
- (viii) Legal.

15. During the Relevant Period from about May 2018, the Divisions of the BFS Group were:

- (a) Products & Technology;
- (b) Corporate Development & Strategy;
- (c) People Culture & Client Experience;
- (d) BFS Central & Operations (which included the Fees and Commissions team); and
- (e) BFS Credit.

16. During the Relevant Period, there was a department within BFS Central or BFS Central & Operations that was variously referred to as 'Credit & Risk', 'Risk & Financial Management' and '**Risk Central**'. Risk Central had several teams, including:

- (a) the BFS Operational Risk Management team (**BORM team**); and
- (b) the Fraud and Financial Intelligence team (**Fraud team**). The Fraud team consisted of the Financial Intelligence Unit and the Fraud Prevention Unit.

17. The functions of the Fraud team were set out in the Fraud Risk Management Framework and included:

- (a) transaction monitoring of retail and high risk products;
- (b) investigations with regard to fraud, advice and other relevant investigations;
- (c) developing fraud risk controls aimed at detecting and preventing fraudulent activities;

- (d) ensuring a review and assessment of fraud risk controls was undertaken on a regular basis;
  - (e) fraud awareness and training;
  - (f) liaison with law enforcement, industry, and regulators; and
  - (g) intelligence with regard to research trends, forecast exposure, predictive analysis, operational risk and industry forums.
18. During the Relevant Period, the heads of the BORM team and the Fraud team reported to the head of Risk Central.
19. During the Relevant Period:
- (a) until about September 2019, Financial Crime Compliance (FCC) was a part of the Compliance Division within RMG and that team had responsibility for anti money laundering and counter-terrorism financing (AML/CTF) anti-bribery and sanctions compliance policies and frameworks;
  - (b) from about September 2019, the FCC department was separated from the Compliance division and became its own RMG division called Financial Crime Risk (FCR); and
  - (c) FCC was not responsible for monitoring transactions for fraudulent activity and reporting such activity to relevant divisions or teams within Macquarie such as to the Fraud Team or the BORM Team, but may (in performing its responsibilities set out at (a) above) have incidentally identified such activity and reported it to AUSTRAC where required.

**D. SCOPE OF ISSUES FOR PROCEEDINGS**

20. This proceeding relates to Macquarie not implementing effective controls to prevent or detect transactions conducted by third party Financial Intermediaries through Macquarie's Bulk Transacting system that were outside the scope of the authority conferred on them that only permitted them to withdraw their fees from their clients' CMAs.
21. The following sections outline:

- (a) Cash Management Accounts;
  - (b) the process by which clients conferred authority types on FIs; and
  - (c) the Bulk Transacting System.
22. Throughout the Relevant Period, Macquarie had in place:
- (a) a risk management framework;
  - (b) measures to monitor for and seek to detect fraud such as in relation to the use of credit card, online or mobile banking (that is, other than monitoring for fraud or misuse of Fees Bulk Transacting); and
  - (c) an Anti-Money Laundering and Counter-Terrorism Financing Program to comply with its obligations under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) and *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No.1)* (Cth).
23. The adequacy and effectiveness of those policies and processes generally is not an issue in dispute in this proceeding. On that basis, those measures are not addressed in any detail in this SAFA.

#### E. CASH MANAGEMENT ACCOUNTS AND THIRD PARTY AUTHORITIES

##### *Cash Management Accounts*

24. During the Relevant Period, Macquarie offered – among other financial products – deposit accounts called ‘Cash Management Accounts’.
25. The functionality of CMAs included that they allowed for the transfer of funds to term deposits, to purchase direct shares, invest in managed funds, to receive investment returns such as dividends and interest, and the payment of fees.
26. Express contractual terms of CMAs were set out in documents headed ‘Product Information Statements’, ‘Further Information Guides’ and ‘Fees, limits and lodgement times’.
27. Macquarie’s computerised central banking system, through which transactions on CMAs were processed, was the ‘Macquarie Investment Management System’, known as MIMS.

28. Amongst other systems, the BFS Group also used 'Siebel', a customer relations management system used by Macquarie to record operational matters relating to accounts, clients and advisers.

***Third Party Authorities***

29. A feature of CMAs was that by way of an arrangement between Macquarie and the account holder (**Customer**), Macquarie enabled the conferral of various levels of third party authority (**TPA**) upon third parties including individuals, financial service professionals (such as financial advisers and accountants) and FIs.
30. During the Relevant Period, there were (broadly speaking) the following four levels of TPA allowing for withdrawals on CMAs:
- (a) Fee Authority – authorising the third party to withdraw their fees from the CMA (**Fee Authority**);
  - (b) Government/Tax Authority – authorising the third party to transfer funds to government departments or agencies;
  - (c) General Withdrawal Authority – authorising the third party to make payments and withdrawals for any purpose; and
  - (d) Authorised Signatory – conferring the authorisations provided for by the General Withdrawal Authority, and also authorising the third party to use the Customer's cheque book, change the Customer's details and close the account.
31. The levels of TPA referred to in paragraph 30 above were designed to allow the Customer to control the level of authority provided to FIs or other third parties.
32. To authorise any of these TPA types (with the exception of the Adviser Limited Third Party Authority), the Customer was required to complete a 'Macquarie Third Party Authority' application form (TPA Application Form) and provide a manual signature.
33. Types of TPA associated with a CMA were recorded against the relevant CMA.
34. TPA Application Forms were completed at the time TPA was granted and this authority remained in place until varied or revoked. Third parties with authority on Customer accounts may have been granted authority using TPA Application Forms that were in place prior to



the Relevant Period and retained that authority under the terms of the form they signed prior to the Relevant Period (to the extent not varied or revoked). The same applies with respect to other forms such as Bulk Transacting Registration Forms and Company and Representative Registration Forms described below. For each of these forms there may have been other types of forms or versions in use before, but which were still valid or applied, during the Relevant Period (to the extent not varied or revoked).

***Documents governing the Relationship between the Customer and Macquarie***

35. The Product Information Statements, TPA Application Forms and Further Information Guides each included express provisions relevant to the treatment of TPAs – including Fee Authorities.
36. The Product Information Statement was expressly part of the CMA contractual terms.
37. As to TPAs, the Product Information Statement identified the distinction between authority types, the Customer’s ability to nominate (to Macquarie) differing third party access rights, and – thereby – Macquarie’s role in maintaining those differing access rights. It also contained language with respect to Macquarie’s responsibility for acts of a customer’s Financial Services Professional, and a warning with respect to unauthorised transactions. It provided:

*This Product Information Statement describes the features of the Macquarie CMA ...*

*Unless your Financial Services Professional is an authorised representative of a Macquarie Group company, no Macquarie Group company is responsible for the acts or omissions of your Financial Services Professional. ...*

***Authorising a third party to access your Account***

*You can appoint another person or company to have access to and operate your Account by completing the Third Party Authority form available online.*

*On that form, you may nominate the type of access rights the third party will have to your Account. This may include:*

- *Account enquiry – enables a third party to enquire on your Account*
- *Fee authority – enables you to authorise a third party such as your Financial Services Professional, should you have one, to withdraw their fees from your Account*

- *Government/Tax payment authority* – enables you to authorise a third party to make payments on your behalf to certain government departments, for example the ATO

- *General withdrawal* – enables a third party to make withdrawals from your Account for any purpose investment or otherwise, and

- *Authorised signatory* – enables a third party to have general withdrawal authority access. In addition, it enables them to close your Account or make changes to your Account such as changing your contact details. This excludes changes to signing instructions on your Account and the appointment of other authorised signatories.

...

### ***Electronic Banking security***

...

*If you find an unauthorised transaction, you suspect that someone has gained access to your Secret Code or is using your Secret Code without your authorisation, or your Secret Code, computer or mobile device get lost or stolen, contact us immediately.*

38. Macquarie also issued a series of TPA Application Forms, to be completed by a Customer in order to confer a TPA upon a third party.
39. During the Relevant Period, the TPA Application Form included – in bold, at the top of the front page:

***Use this form to authorise someone else to operate your account on your behalf and specify the level of authority you wish to give them.***

40. Within section 4, headed ‘Appointment of a Financial Services Company’, the TPA Application Form provided ‘*You can use this section to appoint a company or other third party firm (eg a financial advisory firm, stockbroking firm, accounting firm or administrator) to have access to your account*’ and asked, ‘*What level of authority are you appointing?*’ before listing the distinct authority types available for selection by the customer.
41. Section 7 of the TPA Application Form was headed ‘Terms and conditions’. Clause 7.4 set out a series of indemnities and releases by an account holder with respect to the granting of

a TPA over the CMA, though it was express that Macquarie remained ‘liable for any loss or liability which, by operation of law we cannot exclude’: cl 7.5.

42. Section 7 also included:

**7.13 Fee Authority**

*You authorise your stockbroker or adviser, should you have one, to withdraw their fees from your account using online, electronic and telephone withdrawal services or any other method agreed in writing by us.*

43. From December 2018, the TPA Application Form was slightly amended. The top of the first page now included (in bold):

***Please consider carefully who you appoint as a third party on your accounts as we may follow their instructions as if they were yours. It is important that you understand this risk and carefully consider the level of authority you give to them. Please see section 7 for more information***

44. Section 7 then additionally included (again in bold):

***It is important you understand what level of access you are granting a third party. You can revoke these authorities at any time by contacting us.***

45. During the Relevant Period, Macquarie also provided Further Information Guides. These also included information pertinent to TPAs upon CMAs.

46. In particular, cl 6 was headed ‘*Authorising a third party to access your Account*’. This commenced:

*We offer a facility where you may authorise a company, firm or another person to have access to or withdraw from your Account. There are six types of authority...*

47. Clause 6 then set out certain terms and conditions, including as to ‘levels of authority’: cll 6.15-6.20. Within this, cl 6.16 provided:

***Fee authority***

*You authorise your Financial Services Professional, should you have one, to withdraw their fees from your Account.*

48. The Further Information Guides also included the following express terms:

- (a) *You means you the Account holder(s). Where the context permits it also includes any person carrying out any Account transaction on your behalf, for example a person to whom you have given third party access. cl 1.37;*
- (b) *You acknowledge that Macquarie is entitled to rely on, and you will be liable for, any instructions which are received electronically, which appear to have been duly authorised by you. By providing instructions in this way you acknowledge there is an increased risk of fraud and that you release us from, and agree to reimburse us for, any losses and liabilities arising from any payment or action we (acting reasonably) make in this respect, provided we have acted without fraud and negligence. cl 5.2;*
- (c) *You authorise us to accept any instruction that has not been cancelled by you and notified to us prior to us acting on that instruction. cl 5.5;*
- (d) Below cl 5.5, appeared a box stating '**Please be careful!** There is a risk that fraudulent electronic withdrawal requests can be made by someone who has access to your Account number or Login Details and a copy of your signature. From time to time we may verify these requests with you and reserve the right to change or remove this service.';
- (e) Under a subheading in clause 6 entitled '*General terms which apply to all levels of third party authority*':
- i. *Only you may appoint a third party to access or withdraw from your Account. cl 6.1;*
  - ii. *Subject to these terms and conditions, withdrawals may be for any amount. cl 6.4;*
  - iii. *We may cancel the appointment of a third party as an authority on your Account...: cl 6.7;*
  - iv. *You:*
    - a. *indemnify against all loss, liabilities and costs incurred directly or indirectly as a result of the appointment by you of your Financial Services Professional or any person nominated by them in accordance with clause 6.11*
    - ...
    - d. *release us from all claims and liabilities in connection with any action by your Financial Services Professional or any person nominated by them in accordance with clause 6.11, under their appointment or any payment made from your Account on their instruction.*

*However we remain liable for any loss or liability which:*

- a. arises as a result of our negligence, or*
  - b. by operation of law we cannot exclude: cl 6.13;*
- (f) *Clause 10.2(d) stated: Subject to clause 6, you may nominate another person to have access to your Account through Electronic Banking by completing the appropriate form... You will be liable for any transaction made by an Authorised User within the authority you give to them,*
- (g) *Under subheadings in Cl 10.10, 'Security' and 'Security and Fraud': We are committed to providing the highest quality of financial services within a trusted environment. Please read the Security and Fraud statement (available online) for more information,*
- (h) *Clause 12.1: We may suspend, freeze or block the operation of your Account at any time without notice. The circumstances in which we may suspend, freeze or block the operation of your Account include, without limitation,*
- b. if we reasonably consider that you or any person authorised to act or purporting to act on your behalf is acting fraudulently or in breach of the laws of any jurisdiction*
  - c. if we reasonably believe that your Account is being used in a way that may cause loss to you or us, and*
- (i) *Prior to December 2018: You are liable for all transactions that are carried out with your or an Authorised User's knowledge or consent: cl 10.9.*

49. Finally, from December 2018 there were some changes to the Further Information Guide. Relevantly, the Fee Authority provision (new cl 6.13) featured a warning similar to that referred to in paragraph 47 above. It stated:

***Fee Authority*** – *You authorise your Financial Services Professional to withdraw their fees from your Account. Where you choose to grant this level of authority, we recommend you regularly check your statement of advice, fee disclosure statement or other documentation that sets out your fee arrangement with your Financial Services Professional to ensure the correct amounts are being withdrawn.*

50. The new cl 6.19 referred, for the first time in the contractual documents, to Bulk Transacting:

*Bulk transacting is an administration tool we provide to your Financial Services Professional. The tool helps them efficiently collect fees and make bulk payments from multiple Accounts that they or various Financial Services Professionals working for the same firm may have with us. We only permit this tool where you have provided the required level of authority over your Account to your Financial Services Professional. There are no fees or charges to you for the use of bulk transacting by your Financial Services Professional.*

51. Under that wording appeared a box with an exclamation mark symbol, with the warning '*Please check the transactions on your Account carefully. If you suspect any error or unauthorised transaction please promptly notify us.*'
52. Further terms in Further Information Guide from December 2018 included:
  - (a) *You are not liable for loss arising from Electronic Banking transactions carried out using Login Details without your or an Authorised User's knowledge or consent (unauthorised transactions) that occurs after we have been informed that the security of a Secret Code has been breached: c1 9.9; and*
  - (b) *... you should check your Account records carefully and report to us as soon as you become aware of any payments that you think have been made in error or which were not authorised: c1 9.6(b).*

## F. BULK TRANSACTING

### *General*

53. During the Relevant Period, Macquarie made available a 'bulk transacting' method for effecting transactions on CMAs (**Bulk Transacting**; such transactions, **Bulk Transactions**).
54. Bulk Transacting was an online payment tool offered to certain FIs and their Representatives to help them efficiently collect fees, make bulk payments and make multiple BPAY payments from client CMAs. Bulk Transacting was used by FIs and their Representatives to upload one or more transactions to one or more accounts according to the level of authority they had been granted under a TPA.
55. Macquarie promoted Bulk Transacting to Financial Intermediaries. Macquarie made flyers available to FIs regarding Bulk Transacting, including its use for making 'bulk payments' or 'multi payments'. Bulk Transacting was described to FIs as follows: '*streamlines your administration processes and saves you time so you can focus on your clients.*' Amongst other benefits to

the FI, Bulk Transacting was described as providing as a 'key feature' a '*Seamless transfer of fees*' with '*no need to wait for cheques*'. Other 'key features' described included:

- (a) uploading BPay transactions in bulk '*making processing corporate actions and paying your clients' bills a much simpler and quicker process*';
- (b) '*Efficient external payments – with the appropriate client authority, you can transfer funds on your clients' behalf to other financial institutions overnight*';
- (c) '*Tax payments – with your clients' authority, make client payments directly to the Australian Taxation Office (ATO) to help them at tax time, in particular with managing their SMSFs*'.

#### ***Access to Bulk Transacting***

56. For a Representative to obtain access to Bulk Transacting during the Relevant Period, the following steps were required to be completed:

- (a) A FI was required to register with Macquarie to distribute Macquarie products and obtain access to Macquarie Online (a facility by which users were able to access software containing client data, and transact from a remote location, including using bulk transacting). For this to occur, a Macquarie Company Registration Form had to be completed and signed on behalf of the FI and submitted to Macquarie. Macquarie assigned a "Dealer Code" (sometimes referred to as a Broker Code) to the entity so registered. One firm or entity might have multiple registrations and Dealer Codes.
- (b) Representatives were required to complete and sign a Macquarie Representative Registration Form. Employees, agents or corporate authorised representatives, including financial advisers, paraplanners, accountants and support staff could register as representatives in this way.
- (c) a company registered as set out in paragraph 56(a) and / or (b) was required to complete and sign a Bulk Transacting Registration Form and submit it to Macquarie. On the form the company nominated:
  - (i) one or two employees (who were required to be registered as a Representative) who could authorise, approve and upload Bulk

Transactions either solely or jointly. The nominated employees were also required to sign the form; and

- (ii) the bank account in the name of the company that was to accept client funds from Macquarie.

Macquarie assigned an “Admin Office Code” to the company registered for Bulk Transacting in this way. There might be one Admin Office Code assigned to multiple Dealer Codes.

57. During the Relevant Period, the Macquarie Company Registration Form included the following terms and conditions, which the company agreed to in signing the form:

- (a) *Macquarie is not responsible for the actions of the Company acting either within or outside of its legal authority: cl 8 under heading 'General';*
- (b) *On behalf of itself and its Representatives, the Company must ... only use Macquarie Online for proper purposes associated with Clients and only to the extent permitted by their unrevoked authority: cl 1.B under heading 'Security and privacy';*
- (c) *Unless Macquarie receives prior notice to the contrary, Macquarie will be entitled to:*
  - i. rely on any instructions it receives through Macquarie Online via the Macquarie Access Codes issued to the Company or its Representatives;*
  - ii. assume that for any transaction effected via Macquarie Online, the Company or Representative has the appropriate authority: cl 1.J under heading 'Security and privacy';*
- (d) *The Company accepts full responsibility for any expense, loss or liability (howsoever characterised or caused) incurred by Macquarie, the Company or a Client as a result of the misuse of Macquarie Online by the Company or its Representative(s) (both current and former), and for any breach of these terms, including any failure to immediately notify Macquarie of any breach in relation to data security or privacy: under heading 'Responsibility'; and*
- (e) *'Anything associated with or available through Macquarie Online belongs to Macquarie or other third persons and is protected by intellectual property rights. The Company agrees (on its own behalf and on behalf of its Representatives) not to access, download or otherwise use such property other than as*



*expressly permitted by these conditions, and will be responsible, and indemnify Macquarie accordingly, for any unauthorised use of such property: cl 1 under heading 'Intellectual property'.*

58. The Representative Registration Form included terms which a Representative agreed to by signing the form, which were identical to those set out at paragraphs 57(a) to 57(c) and 57(e) save that:
- (a) the word 'Company' in the term at paragraph 57(a) was replaced with 'Representative';
  - (b) the words 'On behalf of itself and its Representatives the Company must' in the term at paragraph 57(b) was replaced with 'The Representative must'; and
  - (c) the words 'The Company agrees (on its own behalf and on behalf of its Representatives)' in the term at paragraph 57(c) were replaced with 'The Representative'.
59. The Bulk Transacting Registration Form contained terms substantially identical to those in 57(b) and 57(e), agreed to by both the Company and their nominated employees signing the form.
60. Representatives with access to Bulk Transacting were permitted by Macquarie to access Bulk Transacting on any account for which the associated FI had a TPA.
61. Where a Representative or FI obtained access to Bulk Transacting prior to the Relevant Period, they did so under the processes, and by completing the forms, then in place (to the extent not varied or revoked), and they were not required to re-register during the Relevant Period.

***Processing Bulk Transactions***

62. During the Relevant Period, there were various types of Bulk Transacting "template" (being electronic data files):
- (a) Fee Payments template;
  - (b) Government/Tax Payments template;
  - (c) General Withdrawal templates, being:
    - (i) BPAY Payments template;

- (ii) External Multi Payments template;
  - (iii) Consolidated Payments template;
  - (iv) Accelerator to Nominated Account Payments template;
  - (v) Credit File Payments template;
  - (vi) Shares/External Payments template; and
- (d) Legacy templates (being templates replaced by the above templates, but which certain Bulk Transaction users continued to use):
- (i) Dealer template;
  - (ii) Transporter template;
  - (iii) Fee and Share template (or 'FAST template'); and
  - (iv) iBroker template.
63. The replacement of the Legacy templates commenced in about April 2014, as a result of the separation of the fee and shares template and introduction of external payments templates. From at least 13 March 2017, Legacy templates were no longer made available for download by FIs and their Representatives. The legacy templates could still be used by FIs and their Representatives, who had previously downloaded and saved those templates, to process Bulk Transactions during the Relevant Period.
64. To complete a Bulk Transaction using the templates set out in paragraph 62(a) to (c) and (d)(iii) a Representative would:
- (a) first complete a 'template';
  - (b) convert the template to a CSV file and upload that CSV file to Macquarie's Cash Bulk Transacting application within the Adviser Portal for processing;
  - (c) enter a corresponding Macquarie Access Code (**MAC**) (being a Macquarie issued personal identification number) and Vasco security token password;

- (d) the Bulk Transacting application would then convert the template into a single standard format, which MIMS accepted and which included the transaction type;
- (e) each of the Fee Payments, Government/Tax Payments and General Withdrawal templates contained a pre-populated field for the transaction type associated with the template (for example the Fee Payments template pre-populated the transaction type 'F' for 'fee transaction') and the Representative could not choose the transaction type;
- (f) the Legacy 'FAST' template', required the Representative to select the transaction type from predefined fields being either 'F' for 'fee transaction' or 'S' for 'share transaction'; and
- (g) when the template (saved as a CSV file) was uploaded into MIMS and converted into a single standard format, the MIMS system would automatically code the transaction type for each transaction (based on the pre-populated field described above). MIMS would then automatically confirm whether the transaction type matched the relevant FI's level of authority in respect of the relevant CMA. If the transaction type linked to the template selected by the Representative did not match the level of authority held by the relevant FI then MIMS would reject the transaction and it would not be processed.

65. The MIMS system was configured so that:

- (a) A Fee Payments template would only cause transactions to be processed:
  - (i) where the relevant Customers had granted Fee Authority or General Withdrawal Authority to the FI; and
  - (ii) to a single bank account pre-nominated as set out in paragraph 56(c)(ii) above.
- (b) A Government/Tax Payments template would only cause transactions to be processed:
  - (i) where the relevant Customers had granted Government/Tax Authority or General Withdrawal Authority; and

- (ii) to specific bank accounts known to be associated with the Australian Taxation Office and other Government agencies.
  - (c) A General Withdrawal template would only cause transactions to be processed where the relevant Customer had granted General Withdrawal Authority to the FI. Transactions could be made to any bank account.
  - (d) The:
    - (i) External Multi Payment templates could also be used where a FI had Government/Tax Authority;
    - (ii) The Accelerator to Nominated Account Payments template allowed for the payment of funds only to a nominated account; and
    - (iii) No TPA was required for the Credit file template, as this template could only be applied where Macquarie was the recipient of the funds transfer.
  - (e) In relation to the templates referred to at paragraph 64(e), if a user changed the pre-populated nominated transaction type, MIMS would reject the transaction and it would not be processed.
66. The FAST template would only cause transactions to be processed where the relevant Customer had granted Fee Authority or General Withdrawal Authority to the FI and the transaction type selected matched that authority.
67. As to the Legacy templates other than the FAST template:
- (a) these involved the transmission of data using files consisting of a specific format comprising payments instructions as set by the Representative and would only be processed if in this format;
  - (b) the user was required to specify the transaction type as either a Fee transaction; General withdrawal transaction; or Government/tax payment transaction other than in relation to the iBroker template, which was set to General Withdrawal Authority;
  - (c) the Dealer template and the Transporter template would only cause transactions to be processed where the relevant Customer had granted Fee Authority or

General Withdrawal Authority to the FI and the transaction type selected matched that authority;

- (d) the iBroker template would only cause transactions to be processed where the relevant Customer had granted General Withdrawal Authority to the FI and the transaction type selected matched that authority; and
- (e) in relation to the specified transaction type on a Legacy template:
  - (i) a transaction nominated as a general withdrawal transaction could be made to any bank account;
  - (ii) a transaction nominated as a fee transaction could only be made to a single bank account pre-nominated as set out in paragraph 56(c); and
  - (iii) a transaction nominated as a government/tax payment transaction could only be made to specific bank accounts known to be associated with the Australian Taxation Office and other Government agencies.

68. There were no limits placed upon amounts that could be paid through a Fees Bulk Transaction, either in respect of individual transactions or the sum of a number of transactions.

#### **G. ADVISER INITIATED PAYMENTS**

69. During the Relevant Period from 25 November 2016, third parties such as FIs and their Representatives, could seek to initiate an 'Adviser Initiated Payment' (AIP). An AIP was (and is) an Electronic Banking service that enabled a FI or Representative to initiate and complete a payment from a CMA, subject to the Customer authorising the specific payment.

70. After a FI or Representative entered a proposed transaction, the relevant Customer of the CMA would receive a Secure Code by SMS alert to their registered mobile phone number. To complete the transaction, it was then necessary for the Customer to provide the Secure Code to the FI or Representative, who would enter the number electronically.

71. After the AIP was made, the relevant Customer would receive a further SMS alert from Macquarie, and an email, confirming that the payment was complete. At all material times

from the launch of AIP on 25 November 2016, a FI did not need to hold a TPA to use AIP. Each transaction was to be individually authorised by the relevant Customer.

## H. THE \$■■■■ ALERT AND FEE PAYMENTS TEMPLATES

### *The ■■■■ Alert*

72. During the Relevant Period until 3 September 2019, the use of the:

- (a) Fee Payments templates; and
- (b) Legacy templates where the transaction type was listed as ‘Fees’ (noting that the iBroker template could not be used for fee transactions),

automatically generated an email alert for Bulk Transactions if they contained a single transaction greater than \$■■■■ (**\$■■■■ Alert**).

73. \$■■■■ Alerts were generated irrespective of whether the FI had a General Withdrawal Authority or a Fee Authority.

74. For a \$■■■■ Alert to be generated, the Fee Payments template submitted via the Bulk Transacting application had to be processed successfully or partially successfully (a Fee Payments template would be processed partially successfully where some transactions requested in the template were processed and others were not). Fee Payments templates not processed at all – for example, as a result of some other error or exception – would not generate a \$■■■■ Alert.

### *The Development of the ■■■■ Alert and the Fee Payments Template*

75. From late 2012 to early 2014, Macquarie developed and implemented changes to Bulk Transacting, including the introduction of:

- (a) a separate Fee Payments template; and
- (b) a \$■■■■ Alert email.

76. Prior to the introduction of the changes set out at paragraph 75 above:

- (a) Macquarie had no \$■■■■ Alert; and

(b) Payments, including the payment of fees, could be made using Legacy templates such as the FAST template.

77. From late 2012 to early 2014, Macquarie employees engaged in internal communications and produced documents for the purposes of developing and implementing changes to Bulk Transacting, the development of the \$█ Alert and the (separate) Fee Payments template.
78. The BFS Macquarie Adviser Services (MAS) Cash team developed the concept of a MIMS generated email alert, specific to Fees Bulk Transacting, and a separate fees template. One of the intentions of the MAS Cash team was that the separation of the FAST template into a fees template and share template would allow for the email alert in relation to fee transactions. The email alert – which would become the \$█ Alert – was intended by that team to be sent to the Fraud team.
79. The development of a separate fees template, and the \$█ Alert, was intended by the BFS MAS Cash team to mitigate the risk of fraudulent transactions, by FIs acting outside of the Fees Authority granted by a customer.
80. The development of the email alert was directed to mitigating the risk of FIs engaging in unauthorised transactions. A Change Request form, from 17 December 2012 records *“the business objective of this change is to reduce the risk of fraud...”*.
81. In February 2013, the project team developing the email alert reached out to a member of BFS S&O Quality Management & Fraud, providing an extract from a business requirements document headed ‘Change request for Bulk Transacting (with Bulk BPAY)’ that set out formal requirements for the \$█ Alert to be generated for fee transactions (including those transactions effected by the separate Fee Payments template). They sought confirmation that the email alert meets the requirement. The extract did not indicate the intention of the change generally or that the BFS Fraud Team would be the recipient of the email alert, and instead it recorded that the email alert would be sent to a mailing list within BFS MAS. This confirmation was provided.
82. In January 2014 a Fraud Analyst observed that there was limited engagement with their team in relation to the email alerts. The Project Manager stated that details of the files (the subject of the email alerts) could be readily provided by the Fees and Commissions Team. The same member of BFS S&O Quality Management & Fraud who approved the requirements of the email alert, also complained about the engagement and stated “based on my understanding,

the proposed process offers little value.” The project team confirmed that the automated email alerts would not be sent to the Fraud inbox, stating that the “Fees and Commissions team can escalate to [the Fraud Team] when required”. As explained in paragraphs 88 and 90 to 103 below, Macquarie introduced the █████ Alert.

83. The business requirements document for the email alert and the separation of the FAST template were signed off by individuals occupying the following roles:

- (a) BFS MAS P&T Project Manager;
- (b) BFS MAS P&T Product Executive (Cash);
- (c) MOT BFS MAS Senior Manager;
- (d) BFS Risk and Compliance Senior Analyst;
- (e) MOT BFS S&O Project Manager; and
- (f) MOT MAS Senior Manager.

84. The business requirements document for the email alert and the separation of the FAST template were also reviewed by individuals occupying the following roles:

- (a) BFS MAS Test Analyst;
- (b) BFS S&O Adviser/Online Service Consultant;
- (c) BFS MAS Sales and Marketing Campaign Executive;
- (d) BFS MAS Test Analyst;
- (e) BFS MAS P&T Project Manager (Cash Online);
- (f) BFS MOT Senior Manager;
- (g) BFS Business Improvement Analyst;
- (h) BFS MAS COG Developer;
- (i) BFS S&O Fraud Account;
- (j) BFS MAS P&T Product Manager (Cash);



(k) MOT BFS MAS Senior Manager; and

(l) Fraud & Surveillance Manager.

85. On or around 6 March 2014, Macquarie published an internal ‘Knowledge Information Tool’ (**KIT**) document headed ‘Features of Bulk Transacting in Macquarie Access [v1.0].html’, which stated:

*For each fee transaction file where any transaction (successful or not) exceeds \$[REDACTED], an alert email will be sent to the distribution list ‘BFS SO Bulk Transacting Fee File Review’. This is sent to the Fraud Prevention and Detection Team for review, also the Fees and Commissions [sic] team (formerly Adviser Online Services)*

86. Macquarie published the document, and subsequent versions, in both **Salesforce** and **KIT**.
87. **Salesforce** and **KIT** were internal Macquarie platforms accessible to both client facing and operational staff within Macquarie’s BFS Group for the purpose of sharing operational procedures to be followed.
88. In April 2014, Macquarie introduced the \$[REDACTED] Alert and (separate) Fee Payments template.
89. Macquarie subsequently reviewed the ‘Features of Bulk Transacting in Macquarie Access’ document and considered whether any changes were necessary on:

- (a) 16 March 2015;
- (b) 1 April 2016; and
- (c) 1 May 2017.

***The Deployment of the [REDACTED] Alert and Fee Template system***

90. The \$[REDACTED] Alerts were automatically provided to a Microsoft Outlook shared mailbox accessible by the Fraud team. In particular, the \$[REDACTED] Alerts were sent to the ‘BFS SO Bulk Transacting Fee File Review’ distribution list. Since 27 August 2014 the distribution list included the ‘BFS Fraud Prevention and Detection Team’ mailbox. Each member of the BFS Fraud Team had full access to the mailbox.
91. The \$[REDACTED] Alerts were designed to be sent to the BFS Fraud team and the Fees and Commissions team.

92. During the Relevant Period, employees in the Fees and Commissions team were not included on the particular distribution list by which the \$ [REDACTED] Alerts were distributed to the BFS Fraud team.
93. A \$ [REDACTED] Alert included the information as set out in redacted document at **Annexure A** (Example \$ [REDACTED] Alert).
94. During the Relevant Period, transactions conducted through Bulk Transacting and AIP (including Fees Bulk Transactions) were pushed to Macquarie's central 'MIMS' system without passing through any fraud monitoring platforms such as 'PRM' or 'RSA Adaptive', and without any manual checks. 'PRM' and 'RSA Adaptive' were automated fraud detection systems Macquarie had in place, the former operated over credit card transactions and the latter over electronic banking and mobile banking transactions.
95. During the Relevant Period, certain employees of Macquarie such as the Fraud Team and Fees and Commissions Team had access to information stored on MIMS and on Siebel (such as information about accounts and transactions, including transaction narratives and amounts, account holders and third party authorities on accounts).
96. During the Relevant Period, the BFS Fraud Team was able to enquire directly with Customers the subject of the \$ [REDACTED] Alerts, and generally, as to the legitimacy of applicable transactions.
97. Transaction Upload Post Processing Reports (**Transaction Reports**) were generated for each of the 167 unauthorised transactions carried out by Mr Hopkins detailed in section H below. Those Transaction Reports contain certain details of the transactions contained within the bulk transacting file to which they relate, including the narrative and amounts of the transactions. One of the details was a "Reference No". A part of that reference number also appeared in the "File reference" of the Hopkins \$ [REDACTED] alerts. For example, the File reference for the \$ [REDACTED] Alert referred to at paragraph 93 is "QWLP4170" and the associated "Reference No" in the Transaction Report is "4170".
98. Members of the Fees and Commissions Team could access the Transaction Reports if they required access to a record of the transactions effected through a particular Bulk Transacting template.
99. During the Relevant Period, neither the Fraud team nor the Fees and Commissions team had a written practice or procedure in place to review or monitor \$ [REDACTED] Alerts.

100. At all material times during the Relevant Period, Macquarie did not systematically review the \$█ Alerts.
101. There is no documented occasion which has been identified by Macquarie during the Relevant Period of employees of Macquarie having enquired of a Customer as to the legitimacy of a transaction because that transaction was the subject of a \$█ Alert.
102. From 3 September 2019 until 8 October 2020, Macquarie's systems did not generate \$█ Alerts. This was an inadvertent consequence of the decommissioning of a legacy system.
103. During the Relevant Period, and subject to paragraphs 65 to 67, Macquarie's systems otherwise made no provision for specific triggers to detect, identify and assess Fees Bulk Transactions that might give rise to suspicions that the Representative had processed the transaction other than in accordance with the scope of the relevant FI's TPA.

#### I. EVENTS PRIOR TO THE RELEVANT PERIOD

104. In the period from May 2012 to July 2016, employees of Macquarie became aware of a number of instances of IFAs having misused Fees Templates, in that they had used Fees Templates to effect Bulk Transactions where the purpose of the transactions was something other than fees.

##### *Mr Hopkins – 2012*

105. Mr Ross Hopkins was an independent financial adviser. He provided personal financial advice under the financial services licence of, or authorisations granted to, the following entities:
- (a) QWL Pty Ltd (ACN 096 284 383) licensed between 1 January 2004 and 20 September 2021 (between September 2006 and August 2021 Mr Hopkins was the sole director of QWL);
  - (b) QWL Asset Management Pty Limited (ACN 123 121 960) was a corporate authorised representative of QWL Pty Ltd between 16 May 2008 and 22 September 2021 (Mr Hopkins was the sole director of QWL Asset Management Pty Limited); and
  - (c) Raven Capital Pty Ltd (ACN 149 962 649) appointed Mr Hopkins as a financial adviser between 22 November 2012 and 31 July 2016 (Mr Hopkins was a director of Raven Capital between 15 August 2011 and 31 July 2016),

(collectively, the **Hopkins Firms**).

106. Each of these entities through which Mr Hopkins provided financial advice was able to effect transactions on clients' CMAs using Bulk Transacting over the following period:

- (a) QWL Pty Ltd: from about August 2001 to about November 2020, with Mr Hopkins' access to Bulk Transacting being removed on 24 October 2019, see paragraph 197);
- (b) QWL Asset Management from about 2008 to about November 2020, with Mr Hopkins' access to Bulk Transacting being removed on 24 October 2019, see paragraph 197);
- (c) Raven Capital Pty Ltd: from about May 2013 to about August 2016;

While Mr Hopkins acted as a Representative of the Hopkins Firms, Mr Hopkins was not employed by, or an authorised representative of, Macquarie.

107. Between about 31 May 2012 and 5 June 2012, employees of Macquarie identified 31 transactions for about \$1,165,000 dating back to January 2012 carried out by Mr Hopkins on CMAs held by the Hopkins Firms' clients using Fees Bulk Transacting, which appeared to be for non-fee purposes in circumstances where the Hopkins Firms had only been granted Fee Authority and Government/Tax Authority by the relevant clients.

108. On 18 June 2012, an employee of Macquarie spoke with Mr Hopkins, informing him that Macquarie was unable to accept further transactions on clients' CMAs that were not for fees and where he did not hold authority to effect withdrawals from those accounts for any reason other than fees.

109. On 9 August 2012, employees of Macquarie identified a further two transactions for \$65,000 in the same circumstances as described above at paragraph 107 above. The two transactions were reversed that same day.

110. Between about 30 May 2012 to some point in 2014 or 2015 which was after April 2014 (when the \$ Alerts were introduced), Macquarie's A&OS team monitored Bulk Transactions effected by Mr Hopkins. The A&OS team did this by setting up a recurring Microsoft Outlook calendar notification in order to prompt the team to manually review transaction files uploaded by Mr Hopkins on a daily basis.

***Peter McIver of Databank – May 2013***

111. On 17 May 2013, an employee of Macquarie identified that Mr Peter McIver, an IFA whose business was called “Databank”, had used Bulk Transacting to debit funds from CMAs held by his clients for the purpose of investment, in circumstances where Databank only held Fee Authority in respect of those clients. Following this, on about 21 May 2013, an employee of Macquarie had discussions with Mr McIver, in which he informed Mr McIver that in the future, Macquarie would reverse Bulk Transactions if Mr McIver conducted similar transactions in respect of clients for which Databank only held a Fee Authority. On that same day, Mr McIver provided Macquarie with a signed withdrawal request on behalf of one of his impacted clients to effect the transaction.
112. From June to at least August 2013, the A&OS and Fraud teams continued to at least periodically monitor and review transactions submitted by Databank.

***Crofts Financial Services – December 2013***

113. On 6 December 2013, an employee of Macquarie, while liaising with an employee of an IFA (Crofts Financial Services) as to why two particular Bulk Transactions (including one transaction for \$50,000) had not been processed by Macquarie, identified that the Bulk Transactions the IFA had attempted to complete had been conducted using the Fees Template, in circumstances where the purpose of the transactions was not for fees and where the two clients had not granted the IFA a General Withdrawal Authority. The Macquarie employee characterised the conduct as giving rise to the potential for misuse of Bulk Transacting. The Macquarie employee also explained to the Crofts Financial Services employee that only fees transactions are to be processed via a Fees Template.
114. Ultimately, the FI provided a withdrawal request signed by one of those clients to effect the transaction.

***Peter McIver of Databank – March 2014***

115. In March 2014, an employee of Macquarie identified that Mr McIver (of Databank) had again engaged in “improper use” of Bulk Transacting, in that Mr McIver had used Bulk Transacting for the purpose of deducting funds from his clients’ CMA in order to make payments to the ATO, in circumstances where all but one of those clients had only granted Fee Authority to Databank.

116. On or around 19 March 2014, the same employee contacted Mr McIver and highlighted the importance of using the correct file type (i.e. Template) for payment type. He also explained that only “true” fee items should be submitted using a Fees Template. On that same day, a decision was made by Macquarie to ‘continue monitoring Databank activity via Bulk Transacting’, even though the Macquarie employee had assessed that this instance was likely one of ‘genuine error’.

***David Orth of Real Wealth – September 2014***

117. In around September 2014, Macquarie cancelled the access of Mr David Orth and his firm, Real Wealth, to Bulk Transacting. Macquarie did this after employees of Macquarie, including the Head of Financial Intelligence, had identified that Real Wealth had used Fees Bulk Transacting to withdraw funds from clients’ CMAs where the purpose of the withdrawals was other than for payment of fees charged by Real Wealth (where Real Wealth only held a Fees Authority), and Mr Orth and Real Wealth had continued to engage in that conduct after having been informed that use of Fees Bulk Transacting was limited to payments of Real Wealth’s fees. The Head of the Fraud Intelligence Unit subsequently recommended that Real Wealth’s access to Bulk Transacting be terminated forthwith.

***Mr Hopkins – 2015***

118. On 26 May 2015, an employee of Macquarie identified that Mr Hopkins had initiated three withdrawals for \$61,200.50 from Hopkins Firms’ clients’ accounts using a Fee Payments template for Bulk Transacting, in circumstances where those clients had only granted a Fee Authority but the withdrawals appeared, including from the transaction description, to be for a non-fee purpose (being for the purchase of shares). The details of those transactions are referred to in an email between Macquarie employees dated 26 May 2015 and included a transaction for \$50,000 with the narrative ‘ADAIRS IPO’, and two further transactions for \$2,565 and \$8,635.50 with the same narrative ‘NAB ENTITLEMENT OFFER’. In this email, the Macquarie employee noted that the behaviour by Mr Hopkins was ‘not new’ and Bulk Transacting by him was being ‘actively monitored’.

119. On 27 May 2015, employees at Macquarie exchanged emails regarding those transactions by Mr Hopkins and the transactions in 2012 the subject of paragraphs 107 to 110 above. On that same day, a Business Development Manager of Macquarie spoke with Mr Hopkins and informed Mr Hopkins that his access to Bulk Transacting would be removed if he sought to

effect such transactions again. During this conversation, Mr Hopkins and his office manager advised the employee of Macquarie that they would obtain General Withdrawal Authorities for those clients whose transactions had been reversed.

120. On 27 May 2015, an alert was placed on the Seibel profile for Mr Hopkins and QWL Pty Ltd which stated: ‘\*\*WARNED RE: IMPROPER USE OF BULK TRANSACTING. refer to activity 1-CSBDP7 on SID 75006165’. The activity notes which accompanied the alert stated that ‘‘if any further improper user of Bulk Transacting, access is to be revoked with no further warnings’’. The alert on Siebel was visible to the user in a panel titled ‘Alerts’. The alert was placed by the same employee who was involved in identifying the repeated instanced improper use by Mr Hopkins of his Fee Authority between January to August 2012 as well as the further instances in May 2015.
121. On 28 May 2015, Mr Hopkins sent an email to a Business Development Manager at Macquarie, attaching two TPAs that granted General Withdrawal Authority in respect of the clients on whose accounts the three transactions referred to at paragraph 118 above were processed, which enabled those transactions to be processed.
122. The recurring Outlook calendar notification in relation to Mr Hopkins described in paragraph 110 above ceased at some point in 2014 or 2015, some time after the introduction of the \$█ Alerts (as described in paragraph 88 above).

## J. EVENTS DURING TO THE RELEVANT PERIOD

### *Shreeve & Carslake Pty Ltd – July 2016*

123. On 17 July 2016, an employee in the BFS Fraud team, and the Head of Financial Intelligence, were notified of incidents where an IFA, Shreeve & Carslake Pty Ltd (SCPL) had effected Bulk Transactions relying on Fee Authority from clients with CMAs where those transactions did not appear to be for a fee purposes. Employees of Macquarie became aware of these incidents indirectly (rather than due to any targeted monitoring or surveillance of SCPL).
124. On 27 July 2016, the BFS Fraud team employee followed up on the incidents involving SCPL referred to at paragraph 123 above:
  - (a) asking if there was a preferred approach in terms of engaging with SCPL as regards ‘‘their improper use of Bulk transacting’’; and

(b) noting that the BFS Fraud team would typically either seek information and documentation as to the nature of the transactions, or seek signed TPAs from the clients with the appropriate level of authority.

125. Despite the instance being alerted to the BFS Fraud Team, the instances involving SCPL did not involve fraud (and there was otherwise no allegations of fraud).

***Macquarie's conduct during the Relevant Period***

126. In or around July 2016, the BFS Group commenced a "Fraud Prevention Review". Within this, the Head of Cash Product was tasked with reviewing the Bulk Transaction process. Macquarie has no record of the product of this review of the Bulk Transaction process, if any.

127. On 17 October 2016, as part of a "Fraud Control Assurance" process, an employee in BFS Operational Risk asked the Head of Financial Intelligence (also being the head of the Fraud team, and who occupied these roles from 2010 to July 2019) what "controls are in place to identify fraudulent transactions using bulk transacting". Macquarie has no record of Head of Financial Intelligence's response, if any.

128. On 31 July 2017, the Head of Financial Intelligence sent an email to employees in the BFS Group and Risk Management Group (**31 July 2017 Email**), including the Head of Compliance, BFS in RMG (who occupied this role or equivalent from April 2017 to May 2021). The email was copied to others including to the Head of BFS Risk Central (who occupied this role from January 2017 to February 2019, and was then the Head of BFS Non-Financial Risk from February 2019 to April 2023, but whose day-to-day responsibilities did not change in this role), the Head of Deposits & Payments Products, BFS (who occupied this role from February 2017 to present). In his email, the Head of Financial Intelligence:

- (a) identified that because CMAs were being migrated to a new online portal ("eBanking") advisers would be more reliant on AIP and Bulk Transacting following the migration;
- (b) observed that as a new facility, AIP had "controls in place to safeguard client payments via a number of built-in operating mechanisms";
- (c) identified that "Bulk Transacting was initially built to provide a streamlined method for advisers to regularly draw fees and commissions (under authority) from client accounts. The facility was later broadened to allow payments to be made from client



accounts under a more general third party authority. Currently no monitoring is being carried out on bulk transaction payments. The liability of these payments again, lies with the advisor have appropriate authority across the account. Macquarie has however, identified losses (historically) to clients due to inappropriate advisor behaviour... At this point, consideration needs to be given as to the level of oversight/monitoring to be provided for [AIP and Bulk Transacting] (by the online fraud team). That monitoring would (at least initially) consist of manual processes around such activity not only focussing on fraud but also compliance. I would like to get an understanding around the business' (and risks) appetite in this area..."; and

- (d) referred to a review ASIC was conducting in relation to third party activity (such as adviser activity) on CMAs, and noted that from that review it had become evident that ASIC was interested in the level of monitoring financial institutions undertake on clients' accounts that have TPAs, and particular in the behaviour of advisers in relation to such accounts. The Head of Financial Intelligence's reference to a review by ASIC was a reference to the review ASIC undertook that resulted in its publication, on 9 August 2018, of Report 584 – "Improved protections for deposit accounts with third-party access" (**ASIC TPA Review**): see paragraph 149 below.

129. The Head of Deposits & Payments Products in the BFS Group and a recipient of the 31 July 2017 Email raised the email with the Head of Banking Product in the BFS Group and the Executive Director, Head of Product and Technology in the BFS Group on 31 July 2017.

129A. On 11 August 2017, a meeting was held regarding monitoring of AIP transactions and Bulk Transacting. At that meeting:

- (a) The Head of Financial Intelligence indicated that "AIP has seen an increase in transactions, our intention was always to shift away from granular monitoring taking into consideration the liability on the adviser for these trx" and that the Fraud team was seeking guidance from the business as to "how much monitoring we want to do and what our risk appetite is?".
- (b) The Head of Compliance, BFS in RMG suggested that there would be merits in an end to-end review of Macquarie's client/adviser/cash payments and withdrawals process and the risks.
- (c) An employee in the Fraud Team was tasked with writing up information on bulk transacting, usage, previous fraud cases, how it can be exploited or defrauded.
- (d) The Head of Deposits & Payments Products, BFS was also at the meeting.

130. On 10 October 2017, ASIC sent an email to the Head of Compliance BFS in RMG, in relation to the ASIC 584 Review, providing a “high level summary” of its findings and recommendations as relating generally to the banks that had participated in the review. These included that customers did not always receive notification of transactions made by their advisers, and that banks transaction monitoring systems lacked “specific triggers to effectively identify adviser fraud”.
131. On 22 December 2017, a Fraud Analyst in the Fraud Team within the BFS Group (**the Fraud Analyst**) prepared a document, and sent it to the Head of Financial Intelligence, setting out information regarding AIP and Bulk Transacting, with possible suggestions for how to monitor activity (**December 2017 Paper**). The report identified the different types of authority relevant to bulk transacting, including a fee authority, and the various templates used in the bulk transacting system including the fee template. In the report, as regards Fee Authorities for Bulk Transactions on CMAs, the Fraud Analyst:
- (a) noted that \$████ Alerts were sent to an email distribution list titled “BFS SO Bulking Transacting Fee File Review”;
  - (b) stated that BFS SO Bulking Transacting Fee File Review distribution list was sent to the Fraud Prevention and Detection team and the Fees and Commissions team;
  - (c) identified that there was potential for misuse in the form of an IFA moving excessive funds to a fee account and then disseminating those funds;
  - (d) identified that one option was to monitor transactions for “excessive amounts”, and another was to note file references to enable periodic review; and
  - (e) noted that there was a need to identify a trigger that would instigate an investigation or intervention.
132. On 16 January 2018, the Head of Financial Intelligence sent an email to employees in the BFS Group including the Head of Deposits & Payments Products, the Head of BFS Risk Central and Head of Banking Product, as well as employees in the BORM team, attaching a paper entitled “Fraud monitoring on Advisor Initiated Payments (AIP) / Bulk Transacting (BT) Products (**Fraud Monitoring Paper**). In the email, the Head of Financial Intelligence said that the paper identified risks posed under the AIP and Bulk Transacting facilities, and observed that those risks would be heightened by the proposed decommissioning of an

existing Macquarie portal (and the migration to the new eBanking portal). It was noted in the Fraud Monitoring Paper that this may result in additional transactions being processed via Bulk Transacting and AIP facilities.

133. In the Fraud Monitoring Paper, in relation to Bulk Transacting, the Head of Financial Intelligence stated:

- (a) Bulk Transacting (BT) was initially built to provide a streamlined method for advisors to regularly draw fees and commissions (under authority) from client accounts. The facility was later broadened to allow payments to be made from client accounts under a more general third party authority;
- (b) the current levels of authority for BT were Fee/Commission Payment; Tax/Government Payment and General Withdrawal (External Multi Payments);
- (c) referred to “limited manual monitoring” that was carried out in relation to Fees Bulk Transacting (being the \$██████ Alerts);
- (d) observed that Bulk Transacting held inherent risks for a number of reasons, including that, unlike AIP, the client was unlikely to be involved at the time of the transaction and may be unaware of funds moving from their account if the adviser was engaged in improper or nefarious behaviour;
- (e) stated that such a scenario presented the greatest risk to the client, which was evidenced by historical scenarios of adviser misbehaviour causing losses to clients, and that it had previously been difficult to identify fraudulent activity from adviser misconduct because the behaviour appeared identical in both genuine and non-genuine scenarios;
- (f) observed that in the ASIC TPA Review, ASIC had highlighted its expectation that financial institutions increase monitoring; and
- (g) in many circumstances, clients were limited to transfers of \$100k from their own account however an advisor (with TPA) could move unlimited funds from an account, potentially without the client’s knowledge.

134. In the Fraud Monitoring Paper, the Head of Financial Intelligence stated under the heading Future State, and with reference to the different types of authority in subparagraph 133(b), above that:

- (a) authority given to advisors/third parties on these accounts is significant. As such, consideration must be given as to why a third party is permitted greater capacity (in dollar terms) to move funds from an account than that of the client themselves;
- (b) both AIP and Bulk Transactions demanded a combination of manual and automated monitoring to minimise fraudulent behaviour, which would require an injection of resources by Macquarie to facilitate such tasks;
- (c) that for manual monitoring, the use of IBM i2 Suite software, which was a tool currently being used by the BFS Fraud Team, would be the most suitable tool to map the activity of transactions being undertaken within the BT facility. As this type of monitoring would be data heavy, the i2 software could trim data to a manageable level and reveal trends or exceptions. The limitations on this process would include identifying suspicious transactions retrospectively and not in real time. This IBM i2 Suite software included the tool 'Analyst's Notebook', a visual analysis tool featuring network visualisations, social network analysis, and geospatial and temporal views to help uncover connections and patterns in data, and was designed to identify and disrupt criminal, cyber and fraudulent threats;
- (d) AIP should be prioritised (ahead of Bulk Transacting) when advisers were being migrated, that it should be default service for advisers, and that for single transactions, only AIP should be used, stating this was because it included client interaction;
- (e) "Product should initiate a small project team to investigate and implement immediate and ongoing solutions to mitigate fraud exposure to these products" with further consideration to be given to the level of oversight / monitoring to be provided;
- (f) The suggestions regarding the monitoring of Fee and Commission payments were to "Monitor for excessive amounts in either a single txn or over a period of time (i.e 1 x \$100k or multiples over a period of time) (Automated)" and "Periodical reviews on longer term behaviour (such as excessive fees) to be mapped using i2 software (Manual)";
- (g) One suggestion regarding monitoring General Withdrawal payments was to "spot check uploaded files" by running files against a whitelist and through i2 to pick up on behavioural trends (Manual); and

(h) He suggested the team convene before the end of January to target the introduction of control measures by the end of March 2018.

135. On 23 January 2018, the Head of Financial Intelligence sent an email to the Head of Wealth Product and Technology and the COO, Wealth Management, BFS. The email included a statement that "BT needs some enhancement to manage inherent risks as the advisor is able to move client funds (under TPA) without any client interaction in the payment process" and asked if either recipient was aware of a similar product to Bulk Transacting about which enquiries could be made. Both recipients replied that they were not aware of a similar product.
136. On 14 March 2018, the Head of Financial Intelligence sent an email to the Fraud Analyst attaching a copy of the Fraud Monitoring Paper together with some data relating to Bulk Transacting. The email referred to the Fraud Monitoring Paper regarding proposed monitoring, noted there were a number of recommendations and suggestions in the paper, and that the Fraud Analyst was to take a lead role in respect of the proposals in the paper.
137. From March 2018 to May 2018, the BFS Fraud Team undertook analysis of what data fields would be required to progress recommendations from the Fraud Monitoring Paper and requested the retrieval of data from the Data and Analytics Team (**D&A team**). In May 2018, the Head of Financial Intelligence identified that the "primary issue inhibiting progress [for three projects including "Bulk Transacting"] is the lack of capacity source specific data to reach sprint requirements."
138. The "sprint requirements" in the paragraph above refer to a two-week "sprint" which formed part of the "enterprise agile methodology" that Macquarie used to prioritise and execute projects during the Relevant Period. The aim of the methodology was to seek to ensure that the resources of each team were allocated to the projects with the highest business or risk management needs in a particular period. Under the methodology, projects were broken down into 12-week "programming increments" (or **PIs**), which were themselves subdivided into six "sprints" of two-weeks each.
139. From April to June 2018, members of the BFS Fraud Team engaged in correspondence with IBM in relation to the possibility of expanding the team's use of the IBM i2 Suite software Analyst's Notebook and iBase, including in relation to transaction monitoring over Bulk Transacting and AIP and 'Mule Account Analysis', in response to an email received from IBM regarding possibly updating to the latest versions of the software. An email on 16 April

noted that a representative of IBM would make recommendations on “whether there are some better usage practises that can be adopted, or recommend some next steps to deploy the software better... and give an idea of the art of the possible e.g. what are the other banks doing.” Issues were raised regarding the compatibility of various available versions of iBase, and the sizes of the databases that could be used with them, with IBM providing information on these matters.

140. On 7 June 2018, ASIC sent an email to the Head of Compliance, BFS in RMG at Macquarie as part of the ASIC TPA Review. In that email, ASIC:

- (a) expressed concern where AIP was not used for an adviser to initiate a transaction, the client was not notified by Macquarie when the adviser initiates a transaction on the client’s account; and
- (b) stated that ASIC considered it to be particularly important for Macquarie to ensure that all clients, not just those on the AIP system, receive notification of transactions that are initiated by an adviser.

141. ASIC’s email was circulated to the Head of Wealth & Banking Operations, the BFS COO and other BFS Group employees including the Head of Deposits & Payments Products, the Head of BFS Risk Central, and the Head of Financial Intelligence, some of whom made observations about it, including:

- (a) raising a query whether ASIC’s concerns could be addressed by enabling push notifications on CMA transactions;
- (b) raising a query as to why AIP could not be mandated for financial advisers;
- (c) suggesting that AIP could not be mandated for some clients for “accessibility” reasons (such as clients aged over 65), and also that Macquarie did not have mobile phone numbers for some clients; and
- (d) stating that the area Macquarie really needed to consider was Bulk Transacting, for which there was presently no notification provided to clients, and in respect of which Macquarie had around 1,500 users registered.

142. On 25 June 2018, the Head of Financial Intelligence sent an email to a mailbox called “BFS Central”, regarding the project relating to monitoring on Bulk Transacting. The email stated

that limited advancement had been made on the project because it was heavily reliant on another project that had priority. The Head of Financial Intelligence had previously (on 24 May 2018) foreshadowed, in an email he copied to, among others, the BFS COO and the Head of BFS Risk Central, that it might be necessary to pause the project for monitoring of Bulk Transactions because another project needed to be prioritised to meet the expectations of the product and project side of the business.

143. In July 2018, the BORM team conducted a 'Wealth Targeted Review' concerning fraud, which included consideration of the CMA product (**Wealth Targeted Review – Fraud**). The BORM team was separate to the Fraud team. Its role included to assist the BFS Group with risk identification, advise the BFS Group about operational risk, and conduct targeted reviews. This team conducted targeted reviews in order to investigate '*heightened areas of risk or focus areas*', which sometimes included assessment of the appropriateness of the controls operating in a particular area. The Wealth Targeted Review – Fraud was undertaken to assess the design and operating effectiveness of BFS Wealth Management's controls to mitigate the risk of fraud.

144. On 5 July 2018, an employee in the BORM Team (**the BORM Employee**) sent an email to the Head of Financial Intelligence featuring a draft observation and action from the Fraud Monitoring Paper addressing Bulk Transacting. This included:

- (a) "Risks were identified in relation to BT and AIP payments. Specifically:
  - BT payments can be made without client approval, there are no payment limits and no notifications are sent to the client following payment."
- (b) The proposed action to address these risks was identified as convening a project team, who was to prioritise and manage the implementation of the following mandatory risk mitigants:
  - "1. Limit edit and approval capabilities granted to advisers as authorised signatories
  2. Notifications to clients on payments and account detail changes including adviser initiated activities."

145. On 23 July 2018, the Head of Compliance, BFS in RMG sent an email to ASIC, attaching a letter from Macquarie to ASIC, in response to ASIC’s inquiry concerning client notifications for CMAs (see paragraph 140 above). In the letter, Macquarie stated that:

- (a) it “will provide automated customer notifications as a result of adviser initiated transactions” through its mobile banking application, or via SMS where the customer was not registered for the mobile banking application;
- (b) “[t]he threshold over which notifications will be sent will be determined by further analysis of relevant customer data”;
- (c) these processes would be implemented by December 2019, or possibly earlier “depending on changes within our IT delivery program”; and
- (d) the ability to send notifications would be limited to customers who had either registered for Macquarie’s mobile banking application or provided their mobile phone numbers.

146. On 1 August 2018, the BORM Employee issued, by email, a document entitled “**Wealth Targeted Review – Fraud**” to the BFS COO, the Head of BFS Risk Central, the Head of Deposits & Payments Products, the Head of Financial Intelligence and other BFS Group employees. The review assessed the design and operating effectiveness of BFS Wealth Management controls to mitigate the risk of fraud. The scope included amendment of bank account and contact details, detection of changes in account activity and movement of funds and monitoring of transactions. The overall conclusion of the Wealth Targeted Review – Fraud was:

*The control environment is operating effectively however, as indicated by the findings in this report, there are control areas that should be strengthened. Specifically:*

- *Payments generated via Bulk Transacting (“BT”) and Adviser Initiated Payments (“AIP”) present scenarios where payments and account detail changes can occur on client accounts without client notification. ... [four other control areas are also referred to]*

147. The Wealth Targeted Review – Fraud included the following observations, and recommendation actions in respect of such observations:



- (a) Observation Three (“[O3]”) was “Payments generated via Bulk Transacting (“BT”) and Adviser Initiated Payments (“AIP”) present scenarios where transactions can occur on client accounts without client notification. This increases the risk of fraudulent activity not being detected. It included reference to the fact that clients can grant advisers, along with other third parties, varying levels of third party authority (“TPA”) access to their accounts with the available authority levels being authorised signatory, general withdrawal, government / tax payment, fee/ commission payment and account enquiry. As regards Bulk Transactions, it was identified that there was a risk because payments could be made without client approval and without notification being sent to the client following payment, and there were no payment limits. In respect of this, the recommended action (“[A3]”) was to define, document and implement a communication strategy for client payments, which, at a minimum was to include implementation of push notification to clients for payments initiated by advisers. The “owner” of this action was the Head of Deposits & Payments Products, and it was due to be completed by 13 December 2019.
- (b) Observation Four (“[O4]”) was “Fraud detection monitoring over Bulk Transacting and Adviser Initiated Payments requires significant strengthening.”. It was stated that current fraud detection monitoring by the BFS Fraud team in relation to AIP and Bulk Transacting was “limited” and in the case of Bulk Transacting, consisted only of the \$████ Alerts. The proposed action (“[A5]”) was for analysis to be conducted to determine “risk exposure with identified gaps” and provide recommendations as to next steps, including exploring digital solutions “to ensure increased coverage of monitoring and enable timely alerts on accounts with higher risk activity”. The “owner” of this action was the Head of Financial Intelligence, and it was due to be completed by 25 January 2019.
- (c) Observation Seven (“[O7]”) was “Overall end-to-end Fraud control environment needs to be documented to ensure transparency of known gaps and consistent application across BFS”. In relation to this, it was stated that there was “currently no document outlining existing end-to-end fraud controls and risk accepted gaps” across products, which could potentially affect timely impact assessment, ensuring consistency and appropriateness of fraud controls, and business stakeholder understanding of fraud controls and business areas susceptible to heightened exposure of fraud risks. The proposed action (“[A10]”) was to document the end-to-end fraud

control framework outlining critical fraud controls for each business and product. The “owner” of this action was the Head of Financial Intelligence, and it was due to be completed by 25 January 2019.

148. The Review owner was the Head of BFS Risk Central and the BFS Sponsor was the COO, Wealth Management, BFS.
149. On 9 August 2018, ASIC published **Report 584** – “Improved protections for deposit accounts with third party access”, following the ASIC TPA Review. ASIC’s findings, set out in the report, including the following:
- (a) Finding 1 – Application forms play an important role in explaining access levels to customers (p14);
  - (b) Finding 6 – Customers should be notified about adviser-initiated transaction requests by the bank (p17);
  - (c) Finding 7 – Banks should conduct background checks and ongoing monitoring of advisers who use the accounts (p18); and
  - (d) Finding 8 – Monitoring systems could be improved with specific triggers to identify adviser fraud (p19). One example of a such a trigger ASIC identified was for large transfers to an adviser’s account, that do not appear to be reasonable fees for service.
150. On 9 August 2018, the BFS Risk Committee (whose membership during the Relevant Period included the BFS COO, the Head of BFS Risk Central (who chaired), the eight BFS division heads, as well as BFS aligned RMG Operational Risk and RMG Compliance considered the Wealth Targeted Review – Fraud and ASIC Report 584, with the Head of Compliance, BFS in RMG to share the ASIC Report with the Committee.
151. On 20 August 2018, the Head of Deposits & Payments Products sent an email to an Associate in the Payment & Deposits team within the BFS Group (**the Associate**) requesting that the Associate prepare a 'gap analysis' between the findings of Report 584 and what Macquarie then currently offered on the CMA (**Gap Analysis**).
152. On 23 August 2018, the Head of Financial Intelligence sent an email to the Associate in relation to queries raised by the Associate in the course of preparing the Gap Analysis. When explaining CMA account monitoring, the Head of Financial Intelligence stated:

“Short answer is we do very little in each of the areas below except for fees over \$█ where a report is generated and forward to the fraud inbox for review.

We have a project due to begin in PI8 (Sep 2018) to address these issues, specifically around the Bulk Transacting (BT) facility.”

153. On 24 August 2018, the Associate sent an email to members of the BFS Risk, Fraud and Wealth Management Teams, including, the Head of Compliance\_BFS in RMG, the Head of Financial Intelligence, and the Head of BFS Risk Central attaching a Gap Analysis document identifying where, in relation to Macquarie’s CMAs, there was a “gap” between ASIC’s findings in Report 584 as to how such accounts should be set up, operated and overseen, and how Macquarie’s CMAs were set up, operated and overseen. The Gap Analysis included the following matters:

- (a) in respect of Finding 6, it was noted that in relation to bulk transacting, clients were not notified. It was suggested that push notifications be implemented. It stated that consideration should also be given to segmenting bulk transacting users based on business needs (i.e. share settlement) and apply restrictions accordingly;
- (b) in respect of Finding 6 there was a further observation that "AIP had a maximum transaction limit of 100K per day, but bulk transacting had no limit (but requires general withdrawal authority)";
- (c) in respect of Finding 7 it was suggested that Macquarie should select a random sample of advisors and periodically review their transaction requests to ensure they are consistent with customer wishes; and
- (d) in respect of Finding 8, it was noted that “Fees over \$█ are flagged and forwarded to the fraud inbox for review. There is currently a project due to begin PI8 (September 2018) to address these scenarios especially for bulk transacting. However, at the moment very little post transactions checks are performed”. It noted that that Report 584 stated that data analytics may be used to profile risky or unusual transaction behaviours, and it was suggested that this could form a health check for Macquarie to flag fraudulent advisers for escalation.

154. On 27 August 2018, the Fraud Analyst sent an email to a BFS Fraud Investigations Specialist (**the Fraud Investigations Specialist**) and the Head of Financial Intelligence stating that

the IBM i2 Suite had been successfully installed with a view to it being used for fraud monitoring over Bulk Transacting. The Fraud Analyst did an iBase 'deep dive' with a representative from IBM to get training around query writing.

155. On 30 August 2018 the Associate sent the Head of Deposits & Payments Products a revised version of the Gap Analysis document with additional worksheets added that included copies of the Welcome Letter sent to customers including reference to the different third-party authorities that might be granted by customers and the liability clause from the third-party authority form. The following changes had been made to the Gap Analysis circulated in August:

- (a) the comment on Finding 1 had been changed to note that the CMA application form outlined the choice of third party authority but not the consequence, with the action being to review the application form to consider further separation of the third party authority form and ensure the consequences for each authority was simple enough for a customer to understand; and
- (b) the comment on Finding 6 included reference to an additional question regarding whether there should be a limit for bulk transacting, including size and volume per account, noting that the existing limit for a tax file was \$100k with all files have a limit of \$99,999,999.99 per transaction line.

156. On 7 September 2018, the Head of Financial Intelligence sent an email to the BFS COO, the Head of BFS Risk Central, the COO of Central & Operations and the Head of Deposits & Payments Products attaching a document entitled "Fraud Strategy 2018-2020". The attached document identified the threat of "Bulk Transacting (BT)" with the associated challenge identified as "ASIC Paper 584 dictates the need for BFS to more closely monitor the activity of third-party authorities (in particular advisors) across all client accounts".

157. Also on 7 September 2018, the BFS Fraud Analyst sent a copy of a slideshow presentation titled 'Bulk Transacting: Monitoring Project – Sept 2018' to several members of the Fraud team including the Head of Financial Intelligence and the Fraud Investigation Specialist. The presentation, among other matters, outlined that "ASIC have provided guidelines for what is expected around monitoring adviser activity" and stated that "the behaviour we are looking to detect" was IFAs using Bulk Transacting to transfer funds to a personal account, charging excessive fees to clients, or moving funds between client accounts". Under the heading "What

we want to see", the presentation stated that: "Using iBase and Analyst notebook, we are looking to identify scenarios where an IFA may be making payments to their personal account".

158. On 27 September 2018, the Fraud Analyst sent an email to the Head of Financial Intelligence outlining the data required, "based on the three concerns", for monitoring of outgoing and incoming payments via the Bulk Transacting facility that should all be accessible from MIMs. The Fraud Analyst stated that the data will need to be fed directly into iBase/i2 suite for continuous monitoring. The Fraud Analyst asked whether the Head of Financial Intelligence was "able to engage [the D&A Team] for assistance with getting access to the data, and requirements to have this fed directly into the i2 software for analysis."
159. On 5 October 2018, the Fraud Analyst sent an email to the Head of Deposits & Payments Products and a division director in the BFS Group (copying in the Head of Financial Intelligence), referring to a meeting the previous day in relation to the proposed approach for monitoring bulk transacting activity, and seeking guidance around thresholds for the project, including thresholds around fee payments and what may be considered excessive for fees (considering an amount or frequency). It also attached a power point presentation headed "Bulk Transacting Monitoring Project, Oct 2018". The presentation included:
- (a) "Behaviour we are looking to detect: IFA using Bulk Transacting to transfer funds to personal account; IFA charging excessive fees to clients; IFA moving funds between client accounts";
  - (b) "Current State... Payments in excess of \$ [REDACTED] trigger an email to the fraud box (80 for Sept)";
  - (c) "Potential Issue: Indicator for Fee payments is that they are routed via a clearing account – Current date samples suggests IFA's use Fee file for IPO's"; and
  - (d) "Bulk Transacting has high volumes of transactions each day. Data will need to be queried to eliminate noise and reduce false positives".
160. Between 5 October 2018 and 22 October 2018, further emails were exchanged between members of the Fraud team, the Product team and D&A team in relation to the creation of a report showing all transactions processed via transacting Fee or General Withdrawal files. In a 5 October email, the Fraud Analyst stated that "ideally we would like this data to be fed

directly into IBM software, or for a csv, extract to be generated on a regular basis for analysis” monthly. The emails recorded that a data set relating to bulk transacting was extracted in April, but that the Fraud Team was seeking assistance to create 2 reports on a monthly basis to improve the controls on deposit accounts with third party access. Members of the Fraud team were undertaking training in Alteryx (an analytics software) in order to access the data themselves, but a query was raised regarding whether assistance might still be required from the D&A team to build the reports.

161. On 22 October 2018, a Product Manager sent an email to the Head of Deposits & Payments Products and the Head of Product and Technology in BFS seeking their approval for acceptance of risks arising out of the Wealth Targeted Review – Fraud, and attaching a “Risk Acceptance Form” addressing the risks proposed to be accepted. The Risk Acceptance Form identified that the risk appetite being breached was “Deficiency in Critical Control”, and the two risks proposed for acceptance were as follows:
- (a) “Payments generated via BT and AIP can allow payments to occur without client notification following the payment”; and
  - (b) “Authorised signatory advisers can make account detail changes (e.g. including bank details, email address and mobile numbers) without client notification (if email address is the adviser’s email).”
162. The Form referred to the different authority levels as being Authorised Signatory (enabling general withdrawal access, amendment of contact details and account closure), General Withdrawal, Government/Tax Payment, Fee/Commission Payment and Account Inquiry.
163. The reason given for acceptance of the risk concerning the lack of client notification of payments from CMAs was: “Temporary acceptance of risk for Bulk Transaction until the notification solution is implemented by December 2019. In the meantime, we are working with the Fraud team to build a monthly transaction monitoring report for Bulk Transacting.” The form also identified under the heading “Action Plan for controls to be implemented” that fraud monitoring for Bulk Transacting was due to be actioned by December 2018.
164. On 22 October 2018, the Head of Deposits & Payments Products sent an email approving acceptance of the risks. On 24 October 2018, the Head of Product and Technology sent an email approving acceptance of the risks. These emails were circulated to the Head of Banking Product.

165. On 23 October 2018, the Head of Deposits & Payments Products sent an email to the Fraud Analyst in response to the email at paragraph 159 above providing a recommendation as to the thresholds for the bulk transacting monitoring program. The email recommended:

- (a) for “Fee payments: Above \$15k could be considered excessive”; and
- (b) for “General withdrawal: \$40k per transaction more than once a day for a week”, and queried whether these thresholds would result in a huge sample size.

166. Between 5 October 2018 and 25 March 2019, the Fraud Analyst posted various comments in the BFS Central Risk Group Microsoft Planner on the P18 Ongoing Bulk Transacting Monitoring task. These updates were copied to a distribution list which included the BFS COO, the Head of BFS Central Risk, the Head of Financial Intelligence, the Director of Fraud Operations in the Fraud Team, and other BFS employees. The updates included:

- (a) On 5 October 2018, “Meeting held 04/10/2018 with key stakeholders. Requirements have been communicated for thresholds for monitoring. Ticket to be raised with D&A for transaction data by product”;
- (b) On 26 October 2018, that “iBase was to be formally onboarded for use in bulk transaction monitoring. Software has previously been manually installed, however there have been compatibility issues with Microsoft 2016. This is in progress.”;
- (c) On 1 November 2018, “i2 Suite software has been submitted for onboarding via request centre.”;
- (d) On 26 November 2018, “Dependency: Data availability. Power Users module for Alteryx being completed. Once data available for testing, proposal can be drafted.”;
- (e) On 29 January 2019, “Awaiting response from IBM around onboarding of i2 suite.”;
- (f) On 21 February 2019, “IBM have advised of solution for importing, however this interferes with the functionality of Office 365. Support ticket has been raised with IBM to discuss work around.”; and
- (g) On 25 March 2020, “Card will rollover to P110.”

167. In late November 2018 the Gap Analysis was updated to include various actions including:

- (a) adding an alert to section 7 of the TPA form and Section 6 of CMA FIG stating “! It's important you understand what level of access you are granting a third party. You can revoke these authorities at any time by contacting us”;
- (b) that notifications to clients were to be implemented across all payments, with a temporary risk acceptance put in place until the notification solution was built in December 2019; and
- (c) designing bulk transacting fraud monitoring to monitor fee payments above \$15k and general withdrawals of \$20k per transactions more than once a day for a week. The gap analysis included a notation that Fraud Operations were to comment on how to close the gaps in relation to aspects of Findings 7 and 8 regarding monitoring of advisers and transactions.

167A. On 3 December 2018, the Fraud Analyst sent an email to the Head of Financial Intelligence noting that the monitoring project for Bulk Transacting in P18 was marked as “*In Progress – Off Track*”, which meant that it was falling behind plan.

167B. On 18 December 2018, the Fraud Analyst informed a senior fraud analyst in the Fraud Team that the Bulk Transacting monitoring project would now not commence until “*Sprint 4*” of P19, which would be in mid-February 2019.

168. On 14 February 2019, a Product Manager in the Products & Projects Team sent an email to the Head of Banking Product and the Head of Deposits & Payments Products attaching an updated Gap Analysis. The email stated that “Transaction monitoring to include Bulk Transacting – will be in place between Mar-Jun 2019...”. The updated gap analysis contained the following:

- (a) in relation to Finding 1, continued reference to the addition of the alert;
- (b) in relation to Finding 6, reference to a “risk acceptance” being in place until notifications to all clients were implemented across all payments by Dec 2019 as agreed with ASIC; and
- (c) in relation to Finding 7, reference to the fact that bulk transacting was “currently not monitored, however will be in place between P19-10 (Mar – Jun).” In relation to Finding 8, a note that “bulk transacting fraud monitoring report currently in design phase to monitor: 1. Fee payments: Above \$15k 2. General withdrawal: \$20k per



transaction more than once a day for a week.” Beside both of these comments on aspects of Findings 7 and 8 there was a notation that Fraud Operations were to comment on how to close this gap in the period “PI 9 (end of March) – PI10 (end of June)”.

169. On 9 April 2019, the Fraud Analyst sent an email to the Head of Financial Intelligence, attaching a draft paper on Bulk Transaction monitoring. The paper referred to the current levels of authority classifications for bulk transactions as being Fee/Commission Payment, Tax/Government Payment and General Withdrawal. It included the following observations:

- (a) under the heading “Problem Statement”: “There is currently no oversight on the transaction activity by third parties acting on behalf of clients utilising the bulk transacting facility... it was unclear whether the detection of inappropriate usage and behavioural misconduct should be a fraud function or a business risk function, and how this information should be triaged, and what action should be taken”;
- (b) “There is currently no monitoring carried out on BT payments...The only reporting generated against BT transactions relates to the Fee Transaction File whereby any transaction (successful or not) exceeding \$ [REDACTED] creates an alert email...The limited amount of information generated in this file makes it difficult to properly monitor for fraudulent activity”;
- (c) “BT holds inherent risks for several reasons Unlike AIP, the client is unlikely to be involved at the time of the transaction and may be unaware of funds moving from their account if the advisor is engaged in improper or nefarious behaviour. This scenario presents the greatest risk to the client, evidenced by historical scenarios of advisor misbehaviour causing losses to clients. It has previously been difficult to identify fraudulent activity on accounts through advisor misconduct as the behaviour appears identical in both genuine and non-genuine scenarios. i.e. the TPA (with full access upon the account) dials into the MBL portal using identical IP address / device / MAC/password (and token where relevant) to carry out the transaction”; and
- (d) matters to be determined included what monitoring was required on the bulk transacting facility; how the behaviour of third parties was to be monitored, and who would own this process and where a case of misconduct was suspected, how it would be triaged, and how third party misconduct would be defined.

170. On 18 April 2019, the Head of Deposits & Payments Products approved the extension of the risk acceptance which was previously put in place on 22 October 2018. The risk acceptance was extended until 31 December 2019. On 23 April 2019, the Head of Product and Technology in the BFS Group provided his approval to the extension of the risk acceptance.
171. On 29 April 2019, the Fraud Analyst posted a comment in the BFS Central Risk Group Microsoft Planner on the PI10 On Hold Ongoing Bulk Transacting monitoring (Phase 2) task copied to the same distribution list outlined above at [x]. “Compatibility issues with iBase suite and Office 365. IBM are looking at solutions for onboarding of software. Meeting scheduled for 9 May to discuss next steps.”
172. On 3 May 2019, the Fraud Analyst sent an email to the Head of Financial Intelligence, with an updated draft of the paper on Bulk Transaction monitoring. The paper included new sections including a section on work undertaken, monitoring of fees payments and monitoring of advisers moving funds between client accounts. In addition to the content referred to in paragraphs 169 above, the paper included the following:

(a) Under the heading “Work undertaken to date”, the statements:

- i. “Given the large volume of transaction data for bulk transacting, the fraud team has opted to use the i2 suite offered by IBM, to query and present the data through link analysis. This software is currently in the process of being onboarded. The BFS fraud team currently holds 3 software licenses, however following the BFS wide upgrade to Office 365 and Office 2016 there have been compatibility issues.

As at 3 May 2019, this has not been resolved by IBM. This is currently being followed up, with a view to look at alternate solutions if this is no longer feasible.”

- ii. “Prior to the Office 2016 upgrade, there was an initial build of queries to analyse a sample of bulk transacting data. This was undertaken between May–July in 2018. The sample data did not differentiate between the types of bulk payments being processed. Given this, there was considerable complexity to differentiate the transactions, and translate this into the query language for IBM. This meant that an additional data source would need to be fed into the software which listed clearing accounts used for fee payments. Ultimately this

additional data was able to be sourced through Business Objects, however this only differentiated fee payments, from external multi payments.”

- (b) Under the heading “Fee Payments”, the statements that:
- iii. “A process map was developed for fee payments, with a suggestion that threshold values would need to be applied. Following an initial response from product, this was decided at \$15K per month per client. When this was applied to the fee data, the volume of transactions was considerably decreased, however the results still yielded a very high false positive ratio, and no indicators for which payments may have been misconduct. The results provided still would require substantial manual intervention, and decision making based on how the data looked for that adviser. A process map was developed, however has not been implemented. Fee payments has been chosen as the first monitoring piece to be completed, due to the more basic nature of the transactions, when compared with external multi payments.”
- (c) Under the subheading “Current view”, that “The view is to take a different approach with the data, to reduce noise, and find better indicators of potential misconduct.” It was proposed to use some household data by the D&A Team, together with transaction data to better demonstrate changes in behaviour for advisers, as well as provide a comparison across different advisers and dealer groups, with an expectation that there would be fraud team intervention only after escalation from other teams.
- (d) The paper also included a section on the monitoring of Advisers moving funds between client accounts, which did not involve Fees Bulk Transacting, and states that since data was obtained in March 2019, the Fraud team will be able to identify more systemic issues, such as if they see complex arrangements between CMAs, or multiple clients paying into an adviser controlled account. The data had “not been queried to date, due to the IBM software compatibility issues, and dependency on data and analytics”. The “view” was to have alerts trigger over transaction data for a rolling 3 months. Data and Analytics estimated an effort of 2 sprints (4 weeks) to build this capability.
- (e) Under the heading “Next Steps”, the following items appeared: “Prioritisation with data and analytics to combine and build out model combining transaction data and

households; Initial testing on alerts through tableau dashboards - Access has been granted; Alerts data to be fed through i2 suite to show link analysis (Dependency on IBM) – no date of when this will be resolved; Testing and refinement of process once data is available; Refine process/triage maps (Dependent on alert volumes); Roll out process for fee payments (Phase 1); Roll out process for external multi payments (Phase 2).”

173. On 9 May 2019, the Fraud Analyst sent an email to BFS employees including the Head of Wealth and Banking Operations, the Head of BFS Non-Financial Risk (formerly the Head of BFS Risk Central), the Head of Financial Intelligence and an Operational Risk Senior Manager, attaching a presentation entitled “Bulk Transacting Monitoring Project – May 2019” for a meeting to be held that day regarding Bulk Transacting. The Fraud Analyst noted that there was an accompanying paper that she would talk through, which had further detail and which she could distribute following the meeting. The presentation:

- (a) identified under “What we are seeing” that “Bulk Transacting has high volumes of transactions each day. Data will need to be queried to eliminate noise and reduce false positives”;
- (b) identified that “progress to date” included that:
  - (i) “IBM suite was onboarded, however compatibility issues with Office 365/Office 2016 has [sic] arisen”, that a support ticket had been raised with IBM and there were weekly follow-ups on progress; and
  - (ii) there was a “data availability issue” with a “dependency on Fraud Power Users” which had been resolved, with sample data now available;
- (c) identified that it was to be determined “who has ownership of monitoring, and escalation/triage to fraud team”;
- (d) stated that phase one of the project would be to introduce monitoring for fee payments, which would include identifying transactions over a monetary threshold of \$15,000, or excessive fee file, consideration of whether the narrative indicated it was not for fees or misuse of fee file;

(e) included a proposed process map for the monitoring of fee payments by way of a quarterly review, which included steps for analysing transactions including: whether the amount was over \$15,000; whether the account was on a whitelist; whether the narrative was not for a fee (indicating a misuse of the Fee template); whether it was an excessive fee file, and then providing for an alert generated in iBase and/or case generated in the fraud case management system Polonious; and the review of cases by an investigator to determine if intervention was required; and

(f) next steps were to agree on ownership (Payments/Product/BFS Fraud Team), prioritisation with the D&A Team for build, licensing and training on tableau for alerting, process build out and testing and agree on escalation process, and intervention required.

174. On 10 May 2019, the BFS Fraud Investigations Specialist sent an email to the Head of BFS Non-Financial Risk attaching the same paper regarding monitoring for Bulk Transacting as at paragraph 172 above. The paper was also sent to the Director of Fraud Operations on 14 May 2019.

175. From mid-May to August 2019, an Operational Risk Manager in the BORM team within the BFS Group (**the Operational Risk Manager**) conducted a review of Bulk Transacting. During this review input and feedback was provided by members of the Fraud, BFS Risk Central, and Wealth and Banking Operations teams.

176. On 24 June 2019, the Director of Fraud Operations commented in the BFS Central Risk Group Microsoft Planner on the PI10 On Hold Ongoing Bulk Transacting monitoring (Phase 2) which was circulated to the same distribution list outlined above at paragraph 166. This update recorded "Ops Risk review is currently underway, being performed by [the Operational Risk Manager], updated expected by the next meeting".

177. On 23 August 2019, the Operational Risk Manager sent an email to BFS employees including the Head of Deposits & Payments Products, and the Head of BFS Non-Financial Risk attaching a set of slides entitled "Bulk transacting review – Observations" in draft form (**Draft BORM Review**). This was also sent to the Director of Fraud Operations and the Division Director of Governance, Culture, Remuneration and Accountability Review Project on 25 August 2019.

178. The Draft BORM Review and **Final BORM Review** (which was circulated on 18 December 2019: see paragraph 190 below) noted that bulk transacting was offered to external advisors and dealer groups to offer efficiencies in making thousands of payments at once with no fees or charges required to use it. This had resulted in it becoming a very popular offering making up approximately 40% of all CMA transaction volume. The Reviews set out how bulk transacting was effected and noted that it could be used to make fee or tax payments or general withdrawals, with each payment type having a corresponding template to be completed by the advisor and uploaded to the portal. They stated that the BORM Review had “focused on the risks and controls present in the bulk transacting offering”. It noted that the BORM, BFS Legal and the Fraud teams were engaged to ensure all risks and controls were considered.

179. The Draft BORM Review and Final BORM Review included the observations set out below (among others), with action items refined over time and changes made to the persons responsible for those items:

- (a) “Advisers are consistently using bulk transacting to complete single payments: 47% of BT files relate to single payments. 73% of templates are for 5 or less underlying payments. Of the single payments, 79% are general withdrawals. These payments could be facilitated by AIP.” The “opportunity / action” identified by Macquarie in all versions of the Report was to review the potential to push single payments to AIP. The Final BORM Review noted that this was “in progress”.
- (b) “No fraud monitoring is completed over bulk transacting: Bulk transacting payment data does not currently feed into any fraud monitoring system. Alerts are automatically generated by the BT system and sent to the Fraud team where a fee template transaction is >\$█. These are the only alerts generated for the Fraud team and they are not currently actioned.” The opportunity / action identified in the Draft BORM Review was to: “Feed BT payment data into fraud monitoring engine. Establish rules/alerts for investigation”. In the Final BORM Review, this opportunity/action was recorded as being complete, and an additional opportunity/action, to “implement process to review and action reporting”, was to be completed by 10 April 2020.
- (c) “Clients are not notified in real time of any transactions completed on their behalf: There is no real time notification for clients when a payment is made from their account regardless of the size of the payment or where the payment is sent to. The

client is reliant on their account statement for notification of any transactions.” The opportunity / action was to implement client notification process for each transaction processed and this was noted in the Final BORM Review to be in progress.

- (d) “No control exists to stop fee templates being used for other payment types: Fee templates are used to draw funds from CMAs to previously nominated accounts. There is no active control in place to stop an adviser or dealer group from drawing funds and using those funds for things like equities purchases. Anecdotal evidence of this exists.” The opportunity / action was to review the potential to implement a limit on fee template values. The Final BORM Review noted that this was to be completed by 30 June 2020 as part of a proposed solution design for replacing BT.

180. The Draft BORM Review also included the observation that “There is no clear owner or SME for the end to end BT process: There is currently no owner for the entire BT process who understands how the teams and systems interact. If an issue were to be found how would it be managed? How are other changes across BFS considered for impact on BT?” The opportunity / action in the Draft BORM Review was to create a framework for appropriate escalation of issues, change management. This observation was removed from the final version of the BORM Review following the identification of a process owner in an email from Head of Deposits & Payments Products on 16 December 2019.

181. On 27 August 2019, the Director of Fraud Operations sent an email to the Head of BFS Non-Financial Risk and the Fraud Investigations Specialist with the subject: “RE: BFS FCC Governance Forum – August 2019”. The email outlined that in response to the BORM Review Presentation, the initial considerations regarding running the bulk transactions through the fraud engines are that these will not pick up fraud, as the payment is coming from the IFA IP address, and have been authorised via the Vasco token. One option would be that Macquarie “could remove all payment types apart from Fees within Bulk Transactions, and then look for all other payments to be pushed through via AIP – we can discuss the options as part of the meeting”.

182. On 9 September 2019, the Operational Risk Manager circulated an updated version of the Draft BORM Review, in which he had made changes (requested by the Head of Deposits & Payments Products) as to the identification of the Macquarie employee responsible for (referred to as being the “owner” of) particular actions identified in the presentation, including to the Head of BFS Non-Financial Risk and the Head of Deposits & Payments Products.

183. On 18 September 2019, the Head of Deposits & Payments Products responded to an enquiry from the Head of Client Solutions asking about the current position on the use of Bulk Transacting. In her email the Head of Deposits & Payments Products stated that her view was that Macquarie needed to offer some kind of Bulk Transacting ability to advisers. Further, the response stated

“the challenge with the current set up is that 48% of payments going thru Bulk Trans are for single line payments and my hypothesis is that advisers re doing this to get around the SMS that occurs when using AIP.”

184. On 25 September 2019, the Head of Deposits & Payments Products sent an email to the Head of BFS Non Financial Risk, which was sent to the Director of Fraud Operations, within which she stated she was:

“getting increasingly concerned that we don’t have fraud monitoring on AIP and Bulk Transacting. We don’t seem to be able to make any progress with the Fraud team on this matter. Can you help?”

185. From about 18 October 2019 as a result of receiving notices from ASIC dated 17 October 2019, employees of Macquarie reviewed transactions undertaken by Mr Hopkins. As part of its initial review, in an email dated 23 October 2019 a Fraud Analyst of Macquarie identified 114 transactions totalling \$2,221,343.98 in relation to 14 client accounts during 2018-2019 in which Mr Hopkins appeared to have misused his Fees Authority by undertaking Fees Bulk Transactions for purposes other than fees. In an email chain on 24 October 2019 among Macquarie employees (including the Head of Deposits & Payments Products and the Head of Compliance, BFS in RMG, the Fraud Analyst and the Fraud Investigations Specialist):

- (a) a Macquarie employee observed that the total amount withdrawn from client accounts was, on average, over \$158,000 per account, ‘which is much too high for an annual fee’; and
- (b) the Head of Payments & Deposit Products observed that ‘the transaction descriptions [such as ‘QWL.HYBRID.III.PLCMNT.ASX’] on each transaction also points to a transaction other than a fee’.

186. Also on 24 October 2019, as part of the review described in the paragraph above, employees of Macquarie decided to revoke Mr Hopkins’ Bulk Transacting capabilities.



187. Between 5 December 2019 and 9 December 2019, the Fraud Investigations Specialist liaised with a senior manager in the D&A Team in relation to queries to be run across Bulk Transacting payment data to assist in implementing monitoring for external adviser behaviour in Bulk Transacting. The email outlined the 'Name', 'Purpose', 'Key Indicators' and 'Occurrence' for three queries for Fee Transactions Files and two for General Authority Files. The Fraud Investigations Specialist asked for an estimate of how much work was involved and when the senior manager envisaged this could be planned to commence. The senior manager informed the fraud investigations specialist that, while he needed a few days to make sure they would be using the correct data, at a high level and excluding a particular query concerning monitoring of General Authority transactions, the work was '*pretty straightforward*' and would take '*1-2 sprints worth of effort full time*'. As outlined above at paragraph 138, a 'sprint' was two weeks.

188. On 6 December 2019, a member of the BFS Operational Risk team reported to the Head of Deposits & Payments Products and others that the Fraud Team had provided the requirements to build a solution to assist monitoring external advisor behaviour in Bulk Transacting and that the D&A Team had confirmed that the work '*is not overly complex but as always, prioritisation is required*'.

189. On 11 December 2019, the Fraud Investigations Specialist sent an email to the Head of Financial Intelligence attaching a paper entitled "Bulk Transaction – Transaction Monitoring" (dated November 2019). The paper:

(a) reported that the BFS Fraud team had "scoped out" queries that the D&A Team would build and that would be run across Bulk Transacting payment data. The assignment of operational roles and responsibilities for managing and escalating those alerts would then be developed;

(b) In relation to the three Fee Transaction File Queries being developed by the D&A Team:

- i. "Excessive Fees", it was identified that the purpose was detect advisers that are processing a high number of fee transactions through Bulk Transacting that are outside of their normal threshold. The key indicators identified for this were the amount charged to the clients account;

frequency of payments and not in line with other businesses. This was to occur weekly;

- ii. "Misuse of Bulk Transacting Fee File", it was identified that the purpose was to detect where an adviser who only held Fee Authority was processing "general authority" transactions through Bulk Transacting. The key indicators identified for this were "[l]arge transaction amounts" and "[t]ransaction narrative that does not include 'fee'". This was to occur weekly;
- iii. "Credit Transactions in Fee File" – the purpose was to detect where an adviser was processing credit transactions into client accounts through the Bulk Transacting Fee Transaction File. The key indicator was that a "Transaction flag is 'C'". This was to occur weekly.

(c) Two other General Authority File Queries were also developed.

(d) Next steps were noted as being for the Data and Analytics Team to commence work on building the queries commencing December 15<sup>th</sup>, assignment of operational roles and responsibilities for managing and escalating alerts to be developed.

190. On 18 December 2019, the Final BORM Review was sent by the Operational Risk Manager to managers in the BFS team including the Head of Deposits & Payments Products and the COO, Wealth Management, BFS.

191. On 19 December 2019, Macquarie received a report from Deloitte, headed "Deloitte Assessment of Macquarie's Cash Management Accounts Against ASIC Report 584 Recommendations. Within this report, in relation to two of the findings:

- (a) Finding 3 stated: "Our assessment identified that random audits of advisers to review for unauthorised transactions was not conducted";
- (b) Finding 4 stated: "Our assessment identified a number of initiatives which Macquarie are undertaking and implementing to fully address ASIC REP 584, these include: 1. Customers push notifications/SMS for adviser-initiated transactions by January; and 2. Improving the monitoring system of advisers by utilising specific triggers to identify potential instances of adviser fraud by 2020".

192. In late January 2020, Macquarie completed implementation of notifications to alert CMA holders of transactions that had been initiated by an adviser (except in relation to transfers to nominated accounts on Macquarie's wrap platform). Macquarie had communicated to ASIC on 9 December 2019 that it had built the technological solution for push notifications but that it was delaying implementation until before the end of January 2020 to ensure it had the right client communications in place. When the payment was initiated by Bulk Transacting or AIP, CMA holders who had Macquarie's mobile banking app ("mBanking") received a real-time notification, with the transaction details, through that app. CMA holders who did not have mBanking instead received an SMS notification of the transaction. CMA holders could opt out of receiving these notifications by de-selecting the option in mBanking, calling Macquarie's contact centre, or providing written instructions.

***Mr Hopkins' fraudulent conduct – October 2016 to October 2019***

193. Between 14 October 2016 and 8 October 2019, Mr Hopkins fraudulently executed 167 Fees Bulk Transactions on clients' CMAs using the Fee Payments template in circumstances where QWL Pty Ltd or QWL Asset Management Pty Ltd relevantly held only a Fee Authority (and Government / Tax Authority) for the relevant clients and the transactions were outside the scope of the applicable Fee Authority, that is they were not for payment of fees owing to QWL Pty Ltd, QWL Asset Management Pty Ltd or Mr Hopkins. Details of the unauthorised transactions are set out in **Annexure C** to this SOAF. **Annexure C** also identifies:

- (a) in italics, other transactions which were included in the same bulk transaction files as the unauthorised transactions; and
- (b) in underline, other transactions which were included in the same bulk transaction files as the unauthorised transactions, but which were rejected because of insufficient funds in that client's account.

194. By this conduct, Mr Hopkins misappropriated \$2,938,750 from 14 CMAs held by 13 clients. Of those 167 transactions, 97 were the subject of 85 \$ Alerts. In executing the 167 Fees Bulk Transactions, Mr Hopkins used narratives that were inconsistent with use reliant upon a Fee Authority. Rather, the narratives indicated that the transfers were for investment purposes. The bank statements for the relevant customers also contained monthly deductions of between \$211.00 and \$2,887.34 with the transaction descriptions including 'QWL MGT'

FEE'. The frequency or irregularity by which Hopkins executed the 167 Fees Bulk Transactions was inconsistent with the charging of monthly management or advice fees.

195. During the Penalty Period, Mr Hopkins misappropriated \$701,500 from clients' CMAs.
196. The misappropriated funds were transferred into the account nominated by Mr Hopkins as the account for the payment of fees and the funds were used for his own benefit.
197. During the Relevant Period until about 17 October 2019, Macquarie engaged in no targeted monitoring of Bulk Transactions conducted by Ross Hopkins. From about 18 October 2019, Macquarie reviewed transactions by Mr Hopkins as a result of the receipt of ASIC notices dated 17 October 2019. This resulted in the decision to revoke his bulk transacting capabilities on 24 October 2019.
198. On 25 May 2021, Mr Hopkins entered a guilty plea in response to charges of having committed 15 indictable offences of engaging in dishonest conduct in relation to the provision of financial services under ss 1041G and 1311(1) of the Corporations Act, and was convicted of those offences.
199. Mr Hopkins admitted in a statement he made in the criminal proceedings in which he was convicted (and which Macquarie was not a party to) that by entering his guilty plea:
  - (a) he made false representations regarding the nature of the unauthorised transfers in order to conceal his dishonest conduct and avoid detection by an independent portfolio administrator and an accountant engaged by one of his clients;
  - (b) for each of the unauthorised transfers he, via his online access to the CMAs entered misleading transfer descriptions consistent with transfers for investment purposes which would appear in the eventual account statements issued to each client by Macquarie;
  - (c) by entering the transfer descriptions "ASX", "HYBRID" and "PLCMNT", he intended to conceal the true nature of the transfers, which he knew were not authorised, as these descriptions were consistent with descriptions used for legitimate transfers and, therefore, they would appear to a client to be for the purpose of legitimate investments; and

- (d) he engaged in dishonest conduct in relation to the provision of financial services by making those unauthorised transfers and misappropriating the funds.

#### K. EVENTS AFTER THE RELEVANT PERIOD

200. Macquarie designed a fraud monitoring program for Bulk Transacting (**BT Fraud Monitoring Program**) with an initial set of automated transaction monitoring rules operational by the end of May 2020, and further rules implemented in October 2020.
201. The monitoring rules contained in the BT Fraud Monitoring Program are designed to detect various indicators of fraud through the Bulk Transacting facility are set out in full at **Confidential Annexure A**, over which the parties will seek suppression orders at the hearing. These include general monitoring rules for all Bulk Transactions, as well as additional specific rules which apply to Bulk Transactions initiated via a Fee Template. Rules 0 to 3 in **Confidential Annexure A** relate specifically to Fees Bulk Transacting and those rules were put in place as follows:
- (a) The rules now known as Rules 2 and 3 were put in place in May 2020; and
  - (b) The rules now known as Rules 0 and 1 were put in place in October 2020.
202. Of the rules applicable to transactions initiated using the Fee Template, under the BT Fraud Monitoring Program, the significance of Rule 0 was that all single transactions over \$ [REDACTED] which are processed via Fees Bulk Transacting are the subject of an alert. An example of such an alert is set out in Annexure A to this SAFA. This alert was the same as the \$ [REDACTED] Alert except that it was sent to a different email distribution list and Macquarie introduced written procedures for the monitoring, review and investigation of these alerts. All alerts which trigger Rule 0 undergo manual investigation by the Adviser Maintenance Team, and, if necessary, are escalated to the Wealth Distribution Risk Team for further investigation and consideration. The Rule 0 alert and the review of the alert do not rely on the use of IBM i2 Suite or iBase. Subsequent actions can include contacting underlying customers to query the transactions and determine their validity. From 3 September 2019 until 8 October 2020, Macquarie's systems did not generate \$ [REDACTED] Alerts. This was an inadvertent consequence of the decommissioning of a legacy system.
203. In around late 2020 or early 2021, employees of Macquarie undertook a back-book review of all transactions processed between 1 November 2019 to 30 November 2020 using a Fee

Template for over \$ [REDACTED] (**Backbook Review**). The purpose of the review was to identify whether conduct similar to that of Mr Hopkins had been occurring with other financial services professionals. The Backbook Review did not identify any instances of fraudulent transactions.

204. A portion of the period covered by the Back Book Review was a period when Macquarie had implemented push notifications (from mid-January 2020) and also a period when Macquarie had implemented both push notifications and monitoring of Fees Bulk Transacting. No other review of that type to identify fraudulent misuse of Fees Bulk Transacting has been conducted by Macquarie for the entire Relevant Period.

205. Since May 2020 (in regards to at least Rules 2 to 3 at **Confidential Annexure A**) and October 2020 (in regards to all of the rules at **Confidential Annexure A**), Macquarie has undertaken transaction monitoring over Fees Bulk Transacting as outlined in paragraphs 200 to 202 above. Macquarie has informed ASIC that from May 2020 to the date of this SAFA, no instance of fraudulent conduct by an adviser has been identified through this monitoring.

206. In December 2021 to January 2022, Macquarie made ex gratia payments in the sum of \$3,548,824 to 12 of Ross Hopkins' clients who had been impacted by the unauthorised transactions (the remaining one client did not require remediation, as that client had been reimbursed by Mr Hopkins). Macquarie remediated those clients in full, which involved:

- (a) repayment of the amount Mr Hopkins had taken from his customers' accounts (less any recovered by the customer);
- (b) interest on the amount in (a) above, at the greater of the CMA and the RBA cash rate on each day plus 6%, from the date of withdrawal until 10 January 2022; and
- (c) a goodwill payment of \$10,000.

#### **L. OTHER MATTERS**

##### ***CMA Customer base***

207. As at August 2017:

- (a) over half a million customers held a CMA with Macquarie; and

- (b) there was over \$26 billion of funds under management or on deposit in respect of CMA products.

208. CMA customers:

- (a) were mostly advised, (that is, most CMA customers had external financial advisers, self-managed superannuation fund (SMSF) administrators, stockbroking firms or accountants associated with their account). As at August 2017 the proportion was more than 85% of funds under management;
- (b) were generally long term customers;
- (c) were mostly companies or trusts, including SMSFs. These customers comprised more than half of Macquarie's CMA customers; and
- (d) where they were a natural person, had an average age of around 57-60.

209. ASIC found that of the Australian banks it reviewed in Report 584 Macquarie had issued the most adviser-operated deposit accounts in number.

#### ***Volumes***

210. During the Relevant Period, the value of transactions effected using the Fee Payments template ranged from \$173,683,552 to \$476,506,321 per calendar month.

211. Set out at **Annexure B** is data on the volume of Bulk Transactions that were processed each month over the course of the Relevant Period (including the share of transactions using the Fee Payments template). In that annexure, the following data has been set out for each year and month (ie column A and column B):

- (a) **column C**: the total number of all Bulk Transactions that were processed during that month;
- (b) **column D**: the total value of all Bulk Transactions that were processed during that month;
- (c) **column E**: the total number of all Bulk Transactions that were processed using the Fee Payments template during that month;

- (d) **column F:** the total value of all Bulk Transactions that were processed using the Fee Payments template during that month;
- (e) **column G:** the total number of all Bulk Transactions that were processed using the Fee Payments template during that month in respect of FIs that had authority to deduct fees but did not have authority to make transactions for any purpose; and
- (f) **column H:** the total value of all Bulk Transactions that were processed using the Fee Payments template during that month in respect of FIs that had authority to deduct fees but did not have authority to make transactions for any purpose.

212. The table below sets out:

- (a) the number of Adviser Businesses (with Admin Office Codes) and associated Advisers (who were natural person Representatives) (for which there is overlap) who had access to Bulk Transacting during the Relevant Period
- (b) the numbers of relevant TPAs held by FIs with Dealer Codes:



Year	Access to Bulk Transacting		Number Fee Authority only TPAs held by FIs (allocated Dealer Codes)	Number of General Authority only TPAs held by FIs (allocated Dealer Codes)	Number of both General Authority and Fee Authority TPAs held by FIs (allocated Dealer Codes)
	Advisers who could conduct Bulk Transactions on behalf of an Adviser Business	Adviser Businesses registered for Bulk Transacting either as FIs or representatives of FIs (and allocated Admin Codes)			
2015	1,712	1,011	24,486	513,848	33,220
2016	2,051	1,116	25,807	596,132	35,179
2017	2,439	1,223	26,409	636,495	36,572
2018	2,661	1,291	26,880	665,462	37,888
2019	2,760	1,321	27,382	697,156	38,429
2020	2,757	1,330	27,366	732,929	38,306

213. The:

- (a) Fee Payments templates; and
- (b) Legacy templates used where the transaction type was listed as 'Fees';

that were uploaded generated the following \$ [REDACTED] Alerts (by month):

Period	Alerts generated by Fee Payments template and Legacy template
September 2015	90
October 2015	92
November 2015	72
December 2015	81
January 2016	76
February 2016	73
March 2016	67
April 2016	83
May 2016	77
June 2016	92
July 2016	103
August 2016	91
September 2016	86
October 2016	83

Period	Alerts generated by Fee Payments template and Legacy template
November 2016	76
December 2016	83
January 2017	85
February 2017	74
March 2017	107
April 2017	84
May 2017	95
June 2017	129
July 2017	102
August 2017	102
September 2017	96
October 2017	103
November 2017	92
December 2017	75

Period	Alerts generated by Fee Payments template and Legacy template
January 2018	97
February 2018	75
March 2018	89
April 2018	81
May 2018	89
June 2018	112
July 2018	108
August 2018	117
September 2018	79
October 2018	98
November 2018	76
December 2018	91
January 2019	105
February 2019	91

Period	\$█ Alerts generated by Fee Payments template and Legacy template
March 2019	105
April 2019	97
May 2019	97
June 2019	136
July 2019	119
August 2019	103
September 2019	8
October 2019	0
November 2019	0
December 2019	0
January 2020	0

214. After the implementation of Rule 0, Macquarie created a 'whitelist' of adviser groups whose transactions were not required to be manually monitored. The figures in the above table at paragraph 213 include \$█ Alerts in respect of adviser groups who were ultimately whitelisted and whose transactions would not be manually monitored by Rule 0.

**Supplementary Facts – Financial Information**

215. Macquarie's net operating income, net profit after tax, total assets, and net assets in respect of the financial years ending on 31 March in each of 2016 to 2020 are set out in the table below:

<b>FY</b>	<b>Net Operating Income</b>	<b>Net Profit after tax</b>	<b>Total Assets</b>	<b>Net Assets</b>
<b>FY 2016</b>	\$5,643,000,000	\$1,050,000,000	\$181,609,000,000	\$12,710,000,000
<b>FY 2017</b>	\$5,821,000,000	\$1,221,000,000	\$167,441,000,000	\$12,588,000,000
<b>FY 2018</b>	\$5,002,000,000	\$1,023,000,000	\$173,218,000,000	\$13,103,000,000
<b>FY 2019</b>	\$5,911,000,000	\$1,066,000,000	\$163,999,000,000	\$11,240,000,000
<b>FY 2020</b>	\$6,172,000,000	\$1,297,000,000	\$226,136,000,000	\$14,227,000,000

216. Macquarie was at all material times a subsidiary of Macquarie Group Limited (**MGL**), which was listed on the Australian Securities Exchange. MGL's net profit after tax, total assets, net assets and market capitalisation in respect of the financial years ending on 31 March in each of 2016 to 2020 are set out in the table below:

<b>FY</b>	<b>Net Profit after tax</b>	<b>Total Assets</b>	<b>Net Assets</b>	<b>Market Capitalisation</b>
<b>FY 2016</b>	\$2,063,000,000	\$196,755,000,000	\$15,664,000,000	\$22,491,000,000
<b>FY 2017</b>	\$2,217,000,000	\$182,877,000,000	\$17,270,000,000	\$30,700,000,000

FY	Net Profit after tax	Total Assets	Net Assets	Market Capitalisation
FY 2018	\$2,557,000,000	\$191,325,000,000	\$18,180,000,000	\$35,024,000,000
FY 2019	\$2,982,000,000	\$197,757,000,000	\$18,364,000,000	\$44,052,000,000
FY 2020	\$2,731,000,000	\$255,802,000,000	\$21,784,000,000	\$30,388,000,000

217. As at 31 March 2019, Macquarie and its related body corporates had an 'annual turnover' within the meaning of the *Corporations Act 2001* (Cth) of more than \$5,250,000,000.

218. On the basis of the fact above at paragraph 217, the maximum penalty for a single contravention of s 912A(1)(a) by Macquarie for conduct commencing from 13 March 2019 to 15 January 2020 is \$525,000,000.

***Supplementary Facts – Organisational Structure of Macquarie and BFS***

219. The employees in the following roles had the following reporting lines during the respective periods they are each referred to from paragraphs 126 to 192 above (in the section of this document headed "Macquarie's conduct during the Relevant Period"):

- (a) the 'Head of Deposits & Payments Products' reported to the 'Head of Banking Product and Technology', who in turn reported to the 'Head of Product & Technology'. The Head of Deposits & Payment Products was responsible for the product management of various Macquarie products including Cash Management Accounts, Term Deposits, Business Banking Deposits and Credit Cards.
- (b) the 'Head of Wealth Product and Technology' reported to the 'Head of Product and Technology'.
- (c) the 'Director of Fraud Operations' reported:
  - i. from 5 October 2018 to 25 July 2019, to the Head of Financial Intelligence; and

- ii. from 26 July 2019 to 25 September 2019, to the Head of BFS Non-Financial Risk.
- (d) the 'Head of Financial Intelligence' reported to the 'Head of BFS Risk Central' until 9 July 2019. The Head of Financial Intelligence was responsible for the duties of the BFS Fraud Team including to undertake transaction monitoring on high-risk products, undertaking internal and external investigations where needed, liaising with industry and law enforcement, identifying intelligence cells or threats for retail clients, and preparing and providing training and awareness programs.
  - (e) the 'Head of Compliance BFS in RMG' reported within the Compliance Division of RMG, with a secondary reporting line to the 'Head of BFS Risk Central'.
  - (f) the 'Head of BFS Risk Central' (which role later became referred to as the 'Head of BFS Non-Financial Risk' as at 8 February 2019) reported to the 'BFS Chief Operating Officer'. The Head of BFS Risk Central was responsible for the BFS Operational Risk Team and the BFS Fraud Team.
  - (g) 'The Head of Wealth and Banking Operations' reported to the 'Head of Service Sales Centre & Operations' (who in turn reported to the BFS Group Head) until April 2018, and then from April 2018 to the 'BFS Chief Operating Officer'. The Head of Wealth and Banking Operations was responsible for preparing budgets, forecasts and strategies for the Operations Teams and representing the Operations Teams in dealings with other teams and stakeholders in the BFS Group.
  - (h) The 'COO, Wealth Management, BFS' reported to the 'Head of the Wealth Management Division', who reported to the 'BFS Group Head'.
  - (i) The 'Head of Product & Technology' reported to the 'BFS Chief Operating Officer'.
  - (j) The 'BFS COO' reported to the 'BFS Group Head'.
  - (k) The 'BFS Group Head' was the executive of MGL responsible for the BFS Group and reported to the Chief Executive Officer of MGL.

In regards to each of the above employees, any minor changes in role title have not been reflected where there has been no substantive change in that employee's reporting line.



*General Fraud*

220. Macquarie prepared monthly Fraud Dashboard reports as part of its BFS Risk Reports, which were presented at the BFS Risk Committee. These typically included statistics regarding fraud-related incidents, which Macquarie had identified through its fraud monitoring activities, as well as customer complaints and internally identified issues that were referred to the Fraud Team for investigation, by the category of fraud affecting BFS products, the categories of fraud-related incidents, and monthly commentary on fraud-related incidents and investigations across BFS with a focus on emerging trends and particular incidents of concern. The Fraud Dashboards did not expressly use the term 'adviser fraud', but this type of fraud, if it was identified, would be caught by other categories.
221. By way of example, over the Relevant Period, the Fraud Dashboards record:
- (a) 19,781 instances of attempted fraud in the credit card category with an attempted value of approximately A\$31,725,000;
  - (b) 2,323 instances of attempted fraud in the "online" (later renamed retail/online fraud) category with an attempted value of approximately A\$28,342,000;
  - (c) an increase in Macquarie's fraud detection rate for online and mobile banking; and
  - (d) total losses (across all typologies of fraud) of A\$6,270,000.
222. The Fraud Dashboards in the Relevant Period did not expressly refer to the fraudulent misuse of Fees Bulk Transacting by Mr Hopkins or include those customers' losses during the Relevant Period
223. In its Report 584 (referred to at paragraph 149 above), ASIC stated that it had not found widespread misconduct in relation to adviser-operated deposit accounts offered by the banks the subject of its review, but noted that the potential impact of fraud on individual customers was significant. ASIC also found in Report 584 that Macquarie had issued the most adviser-operated deposit accounts in number. In the reports referred to in **Section J** of this SAFA, Macquarie recognised the risk of such misconduct.
224. The only instances of fraudulent misuse of Fees Bulk Transacting that were identified by Macquarie during the Relevant Period were the instances relating to Mr Hopkins.

225. Where misconduct by Financial Intermediaries in relation to adviser-operated accounts occurred, the potential impact on individual customers was significant.

226. Controls relating to the use of Bulk Transacting by Financial Intermediaries included:

- (a) Macquarie had onboarding controls and processes to check the AFSL of FIs and their representatives when they registered with Macquarie, including checking those AFSL holders on a regular basis to ensure they remained appropriately licensed to engage in the services which they sought to provide using Macquarie's products, and to offboard financial advisers who had been banned from practicing.
- (b) As set out at paragraphs 56 to 59 above, FIs and their representatives had to give undertakings to Macquarie in order to gain access to Bulk Transacting.
- (c) There was an onboarding procedure to check that the pre-nominated bank account into which Fees Bulk Transacting payments were made (as outlined in paragraphs 56 and 65(a) above) was in the name of the company that had registered for access to Bulk Transacting.
- (d) Macquarie had processes to ensure a customer had in fact granted a TPA to an FI, and were informed of the nature of the TPA in terms outlined from paragraphs 39 to 52 above. That included a requirement for a customer to fill and sign a TPA form, providing the documents headed 'Product Information Statements', 'Further Information Guides', and issuing welcome letters to the customers setting out the TPAs.
- (e) Macquarie had systems to ensure transactions by an FI were done by an FI's representative and not an unauthorised third party. The portal through which an FI's representative could enter Bulk Transactions required correct login and password details to be entered, along with a six-digit code shown on a physical VASCO token (as set out at paragraph 64 above), which frequently changed.
- (f) Customers could have 24-hour access to their CMA transaction history through electronic banking and mobile banking and bank account statements were made available half-yearly by default or more frequently if requested (which were themselves available online, or mailed to customers if they opted to receive

statements that way). This was explained to customers in the Product Information Statements for the CMA.

***Supplementary Facts – Function of RSA Adaptive***

227. RSA Adaptive (also referred to as RSA Adaptive Authentication or **RSA AA**) was an "off-the-shelf" automated authentication and fraud detection system, that used pre-built transaction monitoring rules which were designed to detect unauthorised access to a client's account (including over CMAs), which Macquarie implemented during the Relevant Period. As set out at paragraph 94 above, transactions conducted through Bulk Transacting were not monitored by RSA AA.

228. There were technical limitations which meant it was not possible from the outset for transactions conducted through Bulk Transacting to be monitored by RSA AA, including because:

- (a) RSA AA was unable to operate on the legacy platform used to process Bulk Transacting files during the Relevant Period.
- (b) RSA AA had pre-built transaction monitoring rules which were not designed to detect fraudulent transactions by advisers who were authorised to access the accounts and had otherwise logged into their accounts normally.

229. A 2015 business requirements document relating to the 'Fraud Management Programme' records that as part of the process of implementing RSA AA, Macquarie had determined that:

- (a) RSA AA should operate to detect Third Party Fraud: ie, fraud occurring without the knowledge of the client whose information is used to commit the fraud (eg, an unknown third party obtaining a client's login details through social engineering, skimming or phishing).
- (b) 'Intermediary Fraud' (ie, fraud committed by an intermediary, such as a customer's adviser or FI) would be out of scope. That decision was made on the basis that Macquarie's assessed that Third Party Fraud presented the highest fraud risk exposure for BFS.

230. Macquarie was unable to identify an "off the shelf" fraud monitoring solution, with pre-set transaction monitoring rules and related data analysis capability, available to address the

general risk of fraud by Financial Intermediaries over the Bulk Transacting facility (such as the fraudulent instances involving Mr Hopkins) (albeit, in regards to Fees Bulk Transacting and the specific risk of advisor misconduct, it was open to Macquarie to manually monitor the \$ Alerts during the Relevant Period). In order to develop a technical solution, Macquarie needed to design bespoke transaction monitoring rules and analysis (see **Confidential Annexure A**).

231. Macquarie encountered technical difficulties in using the IBM i2 Software which it used in designing its transaction monitoring rules, including because the software was not compatible with Microsoft Office 2016 (as described above at paragraphs 158, 160, 166, 169, 171, 172(a) and 172(d) and 173(b)).

#### ***Previous contraventions***

232. Macquarie has not previously been found by any court to have contravened s912A of the *Corporations Act 2001* (Cth), and no court has previously made any declaration that Macquarie has contravened a civil penalty provision under the *Corporations Act 2001* (Cth) or made any order that Macquarie pay a penalty on such a contravention.
233. On 23 August 2016, the Supreme Court of New South Wales found that Macquarie Investment Management Limited (**MIML**) had contravened ss 601FC(1)(b) and 601FC(5) of the *Corporations Act*.<sup>1</sup> At that time, MIML was a subsidiary of both MGL and Macquarie.

#### **Co-operation**

234. On about 22 September 2020, ASIC commenced an investigation into Macquarie regarding its CMA and the conduct of Mr Hopkins in the period October 2016 to October 2019 (the **Investigation**). The Investigation concluded on about 4 April 2022 on the commencement of this proceeding. During the Investigation, Macquarie engaged openly and transparently with ASIC in relation to the Investigation, including: engaging in voluntary meetings with ASIC concerning the investigation and remediation of customers; Macquarie data specialists met with ASIC on a voluntary basis to provide information about the availability and structure of data that could be provided to ASIC; and Macquarie also provided a written submission to ASIC.

---

<sup>1</sup> *In the matter of Macquarie Investment Management Limited* [2016] NSWSC 1184.

235. Since the commencement of this proceeding:

- (a) Macquarie agreed to a statement of agreed facts filed on 24 February 2023;
- (b) Macquarie responded promptly to requests by ASIC for clarification and the production of documents in connection to this proceeding; and
- (c) in March 2024, Macquarie attended a mediation in good faith with ASIC and as part of that process admitted to liability in this proceeding, including by agreeing to the facts and contraventions set out in this document.

**M. CONTRAVENTIONS OF s 912A(1)(a) OF THE CORPORATIONS ACT**

236. For the purposes of the Proceeding, Macquarie makes the following admissions.

237. The CMAs were deposit-taking facilities made available by an ADI in the course of its banking business. As such, they were each a ‘financial product’ within the meaning of s 764A(1)(i) of the Corporations Act. In dealing in CMAs and Fee Authorities, Macquarie provided financial services within the meaning of ss 766A(1)(b) and 766C(1) of the Corporations Act.

238. These financial services were covered by the terms of the AFSL.

239. Further to the matters referred to above, Macquarie admits that:

- (a) Between 1 May 2016 and 12 March 2019, Macquarie failed to do all things necessary to ensure that the financial services covered by its financial services licence were provided efficiently, honestly and fairly, as a result of Macquarie not implementing effective controls to prevent or detect transactions conducted by third parties through Macquarie’s bulk transacting system that were outside the scope of the authority conferred on them that only permitted them to withdraw their fees from their clients’ Cash Management Accounts, such as the fraudulent transactions made by Mr Ross Hopkins. Macquarie thereby contravened s 912A(1)(a) of the Corporations Act.
- (b) Between 13 March 2019 and 15 January 2020, Macquarie failed to do all things necessary to ensure that the financial services covered by its financial services licence were provided efficiently, honestly and fairly, as a result of Macquarie not implementing effective controls to prevent or detect transactions conducted by

third parties through Macquarie's bulk transacting system that were outside the scope of the authority conferred on them that only permitted them to withdraw their fees from their clients' Cash Management Accounts, such as the fraudulent transactions made by Mr Ross Hopkins. Macquarie thereby contravened s 912A(1)(a) and (5A) of the Corporations Act.

-----  
Nicolette Bearup, Litigation Counsel, ASIC  
Solicitor for the Plaintiff  
Date: 16 April 2024



-----  
Michael Hershman, Litigation Counsel, ASIC  
Date: 16 April 2024



-----  
James Campbell, Partner, Allens  
Solicitor for the Defendant  
Date: 16 April 2024

## Annexure A:

## Example \$ Alert

MAC.0501.0004.0088

██████████

---

**From:** BIPUSER@macquarie.com.au  
**Sent:** Thursday, 6 December 2018 2:12 PM  
**To:** BFS SO Bulk Transacting Fee File Review  
**Subject:** Fee payment file - CMH Bulk Transacting processed file exceeded maximum transaction limit

The following CMH Bulk Transacting file has been processed in MIMS and maximum transaction value is greater than \$ ██████████

-----  
 File reference: QWLP4170  
 MIMS processed date and time: 06/12/2018 14:11  
 Admin office: QWL PTY LTD  
 Destination bank account details:  
 - BSB: ██████████  
 - Account Number: ██████████  
 - Account Name: ██████████  
 Total \$ value of file: \$55,000.00  
 No. of transactions in file: 1  
 Maximum transaction value (\$): \$55,000.00  
 No. of transactions greater than \$ ██████ 1

This email and any attachment is confidential. If you are not the intended recipient, please delete this message. Macquarie does not guarantee the integrity of any emails or attachments. For important disclosures and information about the incorporation and regulated status of Macquarie Group entities please see: [www.macquarie.com/disclosures](http://www.macquarie.com/disclosures)

## Example Rule 0 Alert

MAC.0539.0001.0930

**From:** BIPUSER@macquarie.com.au  
**Sent:** Thu, 25 Feb 2021 14:44:04 +1100  
**To:** BFS CO Adviser Maintenance  
**Subject:** Fee payment file - CMH Bulk Transacting processed file exceeded maximum transaction limit

The following CMH Bulk Transacting file has been processed in MIMS and maximum transaction value is greater than \$ ██████████

-----  
 File reference: FEES1734  
 MIMS processed date and time: 25/02/2021 14:43  
 Admin office: FEES & COMMISSIONS  
 Destination bank account details:  
 - BSB: REDACTED  
 - Account Number: REDACTED  
 - Account Name: FEES & COMMS CBT CLEARIN  
 Total \$ value of file: \$313,313.46  
 No. of transactions in file: 6  
 Maximum transaction value (\$): \$130,000.00  
 No. of transactions greater than \$ ██████ 4

This email and any attachment is confidential. If you are not the intended recipient, please delete this message. Macquarie does not guarantee the integrity of any emails or attachments. For important disclosures and information about the incorporation and regulated status of Macquarie Group entities please see: [www.macquarie.com/disclosures](http://www.macquarie.com/disclosures)

**Annexure B: Volume of Bulk Transactions that have been processed each month over the course of the Relevant Period**

A	B	C	D	E	F	G	H
Year	Month	# Transactions – Bulk Transactions	Amount – Bulk Transactions (\$)	# Transactions – Fee template	Amount – Fee template (\$)	# Transactions – Fee template and fee authority	Amount – Fee template and fee authority (\$)
2016	May	87,143	1,295,155,543	51,276	174,804,248	7,049	3,393,396
2016	June	102,715	1,443,890,273	57,996	199,989,916	7,138	3,935,142
2016	July	103,882	1,423,058,304	56,216	195,468,015	8,269	6,535,701
2016	August	101,317	1,639,399,631	50,191	228,296,713	6,792	3,592,347
2016	September	108,303	1,549,344,191	56,820	184,494,095	7,093	3,488,624
2016	October	107,355	1,391,762,079	54,620	227,634,794	8,276	5,634,323
2016	November	107,982	1,858,999,127	51,368	208,708,165	6,814	3,525,329
2016	December	106,355	1,779,424,602	56,906	235,430,031	6,634	4,409,877
2017	January	96,612	1,208,473,710	54,531	194,893,533	7,407	8,074,240
2017	February	107,931	1,741,837,819	53,187	199,836,975	7,186	7,666,342
2017	March	120,486	1,824,401,807	63,703	243,370,271	6,723	8,328,929
2017	April	105,911	1,447,357,819	55,702	173,680,924	8,297	9,366,864
2017	May	114,337	2,015,366,159	55,621	223,712,185	6,798	7,047,198



A	B	C	D	E	F	G	H
Year	Month	# Transactions – Bulk Transactions	Amount – Bulk Transactions (\$)	# Transactions – Fee template	Amount – Fee template (\$)	# Transactions – Fee template and fee authority	Amount – Fee template and fee authority (\$)
2017	June	128,138	2,525,383,854	61,620	233,174,268	6,823	7,460,899
2017	July	125,695	2,060,340,833	64,580	240,835,078	8,221	9,330,022
2017	August	111,421	1,964,859,629	54,101	230,192,561	6,882	8,790,308
2017	September	114,946	1,984,194,799	59,881	365,244,942	6,310	6,269,244
2017	October	126,379	1,916,831,577	63,135	284,480,062	8,210	9,118,657
2017	November	121,884	2,198,591,324	56,413	275,640,178	6,426	6,985,758
2017	December	118,115	2,016,674,170	61,155	476,503,890	6,367	4,281,603
2018	January	115,055	1,556,628,678	60,779	269,294,735	7,849	6,408,691
2018	February	121,205	1,865,711,606	58,580	263,935,825	6,088	3,193,147
2018	March	122,497	2,020,510,850	62,635	426,994,397	6,356	7,853,372
2018	April	118,728	1,902,755,512	59,306	282,831,458	7,546	5,884,069
2018	May	125,351	2,246,228,061	58,842	307,202,602	6,140	3,828,136
2018	June	130,312	2,221,765,340	63,401	280,644,496	6,268	4,679,218
2018	July	126,674	2,059,947,475	60,574	338,773,223	7,199	5,803,804

A	B	C	D	E	F	G	H
Year	Month	# Transactions – Bulk Transactions	Amount – Bulk Transactions (\$)	# Transactions – Fee template	Amount – Fee template (\$)	# Transactions – Fee template and fee authority	Amount – Fee template and fee authority (\$)
2018	August	122,743	2,241,147,104	57,634	333,302,707	5,867	3,977,618
2018	September	113,289	1,903,852,919	59,841	294,680,202	5,573	3,382,793
2018	October	131,925	2,160,745,452	63,171	300,002,747	6,953	5,593,708
2018	November	110,491	1,800,048,507	54,060	271,826,198	5,177	2,804,066
2018	December	112,077	2,076,733,703	58,749	300,766,969	5,562	3,335,942
2019	January	109,417	1,474,184,301	58,103	279,459,028	6,258	5,120,686
2019	February	112,676	1,926,116,848	53,852	360,601,832	4,722	2,685,829
2019	March	116,839	2,108,121,731	58,764	350,468,874	4,920	3,397,671
2019	April	117,153	1,968,843,038	56,412	334,868,533	5,820	4,405,330
2019	May	135,704	2,459,900,286	65,974	370,247,162	5,473	4,054,765
2019	June	127,172	2,559,351,927	60,515	370,509,072	5,263	4,105,980
2019	July	136,686	2,646,082,144	63,825	444,007,449	6,934	6,593,830
2019	August	119,956	2,463,327,965	51,712	321,395,976	4,775	2,793,876
2019	September	119,707	2,199,016,894	57,750	370,955,627	4,673	3,143,818

A	B	C	D	E	F	G	H
Year	Month	# Transactions – Bulk Transactions	Amount – Bulk Transactions (\$)	# Transactions – Fee template	Amount – Fee template (\$)	# Transactions – Fee template and fee authority	Amount – Fee template and fee authority (\$)
2019	October	143,398	2,477,073,988	66,820	385,183,937	6,425	5,982,764
2019	November	123,003	2,454,326,103	53,295	354,126,500	4,627	3,061,750
2019	December	124,388	2,342,196,592	58,870	315,177,636	4,677	3,342,783
2020	January	65,622	775,312,374	32,948	150,082,281	3,363	2,537,112

**Annexure C: The Hopkins Conduct - the 167 Fees Bulk Transactions grouped by use of a Fee Payments Template**

No.	Date	Transaction Narrative	Hopkins Client	Amount	\$ Alert?
1.	14/10/2016	QWL.PLCMNT	VL	\$26,055	
2.	21/10/2016	QWL.PLCMNT	VL	\$24,445	
3.	01/11/2016	QWL.PLCMNT	VL	\$14,500	
4.	01/11/2016	QWL.PLCMNT	JL	\$12,500	
5.	10/11/2016	QWL.PLCMNT	JL	\$5,000	
6.	29/11/2016	QWL.PLCMNT	JL	\$15,000	
7.	06/12/2016	QWL.PLCMNT	JL	\$15,000	
8.	30/12/2016	QWL.PLCMNT	JL	\$3,650	
9.	03/01/2017	QWL.PLCMNT	TD	\$25,000	
10.	06/01/2017	QWL.PLCMNT	TD	\$5,000	
11.	01/02/2017	QWL.PLCMNT	KP	\$11,000	
			TD	\$11,000	
12.	03/02/2017	QWL.PLCMNT	KP	\$1,100	
13.	03/02/2017	QWL.PLCMNT.ASX	KP	\$10,000	
14.	01/03/2017	QWL.PLCMNT	KP	\$15,000	

No.	Date	Transaction Narrative	Hopkins Client	Amount	\$ Alert?
15.	03/03/2017	QWL PLCMNT	JL	\$4,400	
16.	07/03/2017	QWL PLCMNT	JL KP	\$5,500 \$6,500	
17.	27/03/2017	QWL PLCMNT	JL	\$20,000	
18.	03/04/2017	QWL PLCMNT	JL KP	\$12,500 \$12,500	
19.	07/04/2017	QWL.PLCMNT.ASX	JL KP	\$7,750 \$7,750	
20.	13/04/2017	QWL PLCMNT	JL	\$10,000	
21.	03/05/2017	QWL.PLCMNT.ASX	JL	\$17,500	
22.	05/05/2017	QWL.PLCMNT.ASX	JL	\$5,000	
23.	25/05/2017	QWL.PLCMNT.ASX	JL	\$5,500	
24.	01/06/2017	QWL.PLCMNT.ASX	JL	\$45,000	
25.	15/06/2017	QWL PLCMNT FY17 TAX	JL VL	\$12,500 \$625	
26.	20/06/2017	QWL.PLCMNT.ASX	VL	\$13,875	
27.	23/06/2017	QWL.PLCMNT.ASX	VL	\$17,500	

No.	Date	Transaction Narrative	Hopkins Client	Amount	\$ Alert?
28.	27/06/2017	QWL.PLCMNT.ASX	VL	\$15,000	
29.	29/06/2017	QWL.ASX.PLCMNT	JL	\$12,500	
30.	07/07/2017	QWL.ASX.PLCMNT	JL	\$34,500	
31.	31/07/2017	QWL.PLCMNT	JL	\$5,000	
32.	03/08/2017	QWL.PLCMNT.ASX	JL	\$20,500	
33.	28/08/2017	QWL.ASX.PLCMNT	JL	\$21,000	
34.	29/08/2017	QWL.PLCMNT.ASX	VL	\$6,500	
35.	01/09/2017	QWL.PLCMNT.ASX	VL	\$18,500	
36.	04/09/2017	QWL.PLCMNT.ASX	VL	\$12,750	
37.	22/09/2017	QWL.ASX.PLCMNT	VL	\$15,000	
38.	28/09/2017	QWL.PLCMNT.ASX	VL	\$25,000	
39.	06/10/2017	QWL.PLCMNT.ASX	VL	\$26,500	
40.	26/10/2017	QWL.PLCMNT.ASX	VL	\$20,000	
41.	01/11/2017	QWL.PLCMNT.ASX	VL	\$27,500	
42.	07/11/2017	QWL.PLCMNT.ASX	VL	\$15,000	
43.	17/11/2017	QWL.PLCMNT.ASX	VL	\$10,000	

No.	Date	Transaction Narrative	Hopkins Client	Amount	\$ Alert?
			VL	\$10,000	
44.	29/11/2017	QWL.PLCMNT.ASX	VL	\$20,000	
45.	04/12/2017	QWL.PLCMNT.ASX	VL	\$15,000	
46.	21/12/2017	QWL.PLCMNT.ASX	JL	\$10,000	
47.	27/12/2017	QWL.PLCMNT.ASX	TD	\$5,500	
48.	29/12/2017	QWL.PLCMNT.ASX	VL	\$25,000	
			VL	\$25,000	
49.	12/01/2018	QWL.PLCMNT.ASX	VL	\$24,500	
			VL	\$26,500	
50.	02/02/2018	QWL.PLCMNT.ASX	KP	\$5,000	
			VL	\$7,000	
			VL	\$3,000	
51.	26/02/2018	QWL.PLCMNT.ASX	TD	\$1,750	
52.	28/02/2018	QWL.PLCMNT.ASX	VL	\$20,000	
			KP	\$21,500	
53.	20/03/2018	QWL.PLCMNT.ASX	KP	\$21,750	
54.	28/03/2018	QWL.PLCMNT.ASX	TD	\$30,000	
55.	29/03/2018	QWL.PLCMNT.ASX	VL	\$10,000	

No.	Date	Transaction Narrative	Hopkins Client	Amount	\$ Alert?
56.	29/03/2018	QWL.PLCMNT.ASX	KP	\$10,000	
57.	09/04/2018	QWL.PLCMNT.ASX	KP	\$8,500	
58.	11/04/2018	QWL.PLCMNT.ASX	RS RS BM MB <u>TD (transaction was rejected because of insufficient client funds)</u>	\$40,000 \$50,000 \$50,000 \$15,500 <u>\$25,000</u>	
59.	12/04/2018	QWL.PLCMNT.ASX	TD	\$25,500	
60.	02/05/2018	QWL.PLCMNT.ASX	VL KP TD RS	\$5,000 \$10,000 \$10,000 \$10,000	
61.	08/05/2018	QWL.PLCMNT.ASX	TD KP	\$2,000 \$3,000	
62.	22/05/2018	QWL.PLCMNT.ASX <i>QWL MGT FBE</i>	TD LB	\$2,500 \$375	
63.	25/05/2018	QWL ASX PLCMNT <i>Tax FY18</i>	JL WH	\$5,800 \$3,740	



No.	Date	Transaction Narrative	Hopkins Client	Amount	Alert?
		<i>Tax FY17</i>	<i>WH</i>	<i>\$2,750</i>	
64.	28/05/2018	QWL.PLCMNT.ASX	RS	\$25,000	
65.	04/06/2018	QWL.PLCMNT.ASX	RS KP	\$5,000 \$5,000	
66.	08/06/2018	QWL.PLCMNT.ASX	AH	\$5,250	
67.	12/06/2018	QWL.PLCMNT.ASX	RS	\$9,500	
68.	18/06/2018	QWL.PLCMNT.ASX	AH	\$26,500	
69.	25/06/2018	QWL.PLCMNT.ASX	RS	\$3,000	
70.	29/06/2018	QWL.PLCMNT.ASX	RS	\$45,000	
71.	13/07/2018	QWL.PLCMNT.ASX	AH	\$5,000	
72.	24/07/2018	QWL.PLCMNT.ASX	RS	\$6,750	
73.	30/07/2018	QWL.PLCMNT.ASX	AH	\$15,000	
74.	02/08/2018	QWL.PLCMNT.ASX <i>FY17 ACCGT</i>	RS <i>MB</i>	\$17,500 <i>\$2,750</i>	
75.	08/08/2018	QWL.PLCMNT.ASX	AH	\$3,750	
76.	09/08/2018	QWL.PLCMNT.ASX	RS	\$1,250	
77.	14/08/2018	QWL.PLCMNT.ASX	AH	\$15,000	

No.	Date	Transaction Narrative	Hopkins Client	Amount	\$ Alert?
78.	16/08/2018	QWL.PLCMNT.NOTES.ASX	CR	\$25,000	
			RS	\$50,000	
			BM	\$50,000	
			MB	\$25,000	
79.	21/08/2018	QWL.PLCMNT.ASX	AH	\$5,000	
80.	28/08/2018	QWL.PLCMNT.ASX	LB	\$7,500	
81.	31/08/2018	QWL.PLCMNT.ASX	LB	\$17,500	
82.	07/09/2018	QWL.PLCMNT.ASX	LB	\$18,500	
83.	13/09/2018	QWL.PLCMNT.ASX	AH	\$9,500	
84.	19/09/2018	QWL.PLCMNT.ASX	LB	\$2,750	
85.	20/09/2018	QWL.HYBRID.PLCMNT.ASX	AH	\$11,000	
86.	24/09/2018	QWL.PLCMNT.ASX	LB	\$5,000	
87.	26/09/2018	QWL.PLCMNT.ASX	RS	\$3,000	
88.	28/09/2018	QWL.HYBRID.PLCMNT.ASX	JW	\$12,000	
89.	08/10/2018	QWL.PLCMNT.ASX	LB	\$25,000	
90.	17/10/2018	QWL.PLCMNT.ASX	AH	\$6,500	
91.	22/10/2018	QWL.PLCMNT.ASX	LB	\$2,500	

No.	Date	Transaction Narrative	Hopkins Client	Amount	\$ Alert?
92.	24/10/2018	QWL.PLCMNT.ASX	AH	\$5,000	
93.	01/11/2018	QWL.PLCMNT.ASX	LB	\$50,000	
94.	07/11/2018	QWL.HYBRID.PLCMNT.ASX	JW	\$13,000	
95.	15/11/2018	QWL.PLCMNT.ASX	LB	\$2,550	
			RS	\$2,550	
96.	21/11/2018	QWL.PLCMNT.ASX	LB	\$25,000	
97.	28/11/2018	QWL.HYBRID.II.PLCMNT.ASX	JW	\$12,500	
			MB	\$9,500	
			AW	\$15,000	
98.	04/12/2018	QWL.PLCMNT.ASX	LB	\$150,000	
99.	06/12/2018	QWL.PLCMNT.ASX	LB	\$55,000	
100.	07/12/2018	QWL.HYBRID.III.PLCMNT.ASX	JW	\$12,500	
			MB	\$4,500	
			AW	\$25,000	
101.	13/12/2018	QWL.HYBRID.PLCMNT.ASX	AW	\$17,500	
102.	19/12/2018	QWL.HYBRID.PLCMNT.ASX	MB	\$4,000	
103.	03/01/2019	QWL.PLCMNT.ASX	LB	\$5,000	
104.	07/01/2019	QWL.PLCMNT.ASX	LB	\$17,500	

No.	Date	Transaction Narrative	Hopkins Client	Amount	\$ [REDACTED] Alert?
105.	10/01/2019	QWL.PLCMNT.ASX	JW	\$10,000	[REDACTED]
106.	16/01/2019	QWL.PLCMNT.ASX	LB	\$2,525	[REDACTED]
107.	21/01/2019	QWL.PLCMNT.ASX	LB	\$17,500	[REDACTED]
108.	25/01/2019	QWL.PLCMNT.ASX	AW	\$15,000	[REDACTED]
109.	05/02/2019	QWL.PLCMNT.ASX	LB	\$3,500	[REDACTED]
110.	08/02/2019	QWL.PLCMNT.ASX	LB	\$28,500	[REDACTED]
111.	13/02/2019	QWL.PLCMNT.ASX	LB	\$3,550	[REDACTED]
112.	18/02/2019	QWL.PLCMNT.ASX	JW	\$18,500	[REDACTED]
113.	25/02/2019	QWL.PLCMNT.ASX	AW	\$12,500	[REDACTED]
114.	04/03/2019	QWL.HYBRID.PLCMNT.ASX	CR	\$15,000	[REDACTED]
115.	07/03/2019	QWL.PLCMNT.ASX	LB	\$7,750	[REDACTED]
116.	13/03/2019	QWL.PLCMNT.ASX	JW	\$12,500	[REDACTED]
117.	22/03/2019	QWL.PLCMNT.ASX	AW	\$12,000	[REDACTED]
118.	29/03/2019	QWL.PLCMNT.ASX	AW	\$16,500	[REDACTED]
119.	03/04/2019	QWL.PLCMNT.ASX	AW	\$25,000	[REDACTED]
120.	09/04/2019	QWL.PLCMNT.ASX	AW	\$13,500	[REDACTED]

No.	Date	Transaction Narrative	Hopkins Client	Amount	\$ Alert?
			JW	\$5,000	
121.	15/04/2019	QWL.PLCMNT.ASX	AW	\$17,500	
122.	24/04/2019	QWL.PLCMNT.ASX	JW	\$14,000	
123.	01/05/2019	QWL.PLCMNT.ASX	AW	\$21,500	
124.	07/05/2019	QWL.PLCMNT.ASX	AW	\$15,000	
125.	14/05/2019	QWL.PLCMNT.ASX	AW	\$10,000	
126.	22/05/2019	QWL.PLCMNT.ASX	AW	\$16,500	
127.	30/05/2019	QWL.PLCMNT.ASX	AW	\$40,000	
128.	17/06/2019	QWL.PLCMNT.ASX	AW	\$50,000	
129.	26/06/2019	QWL.PLCMNT.ASX	AW	\$30,000	
130.	28/06/2019	QWL.HYBRID.PLCMNT.ASX	AW	\$25,000	
131.	08/07/2019	QWL.PLCMNT.ASX	AW	\$30,000	
132.	15/07/2019	QWL.PLCMNT.ASX	AW	\$10,000	
133.	01/08/2019	QWL.PLCMNT.ASX	AW	\$30,000	
134.	07/08/2019	QWL.PLCMNT.ASX	AW	\$30,000	
135.	14/08/2019	QWL.PLCMNT.ASX	AW	\$85,000	

No.	Date	Transaction Narrative	Hopkins Client	Amount	\$ [REDACTED] Alert?
136.	16/08/2019	QWL.PLCMNT.ASX	AW	\$65,000	[REDACTED]
137.	30/08/2019	QWL.PLCMNT.ASX	AW	\$37,500	[REDACTED]
138.	13/09/2019	QWL.PLCMNT.ASX	AW	\$35,000	[REDACTED]
139.	26/09/2019	QWL.PLCMNT.ASX	AW	\$25,000	[REDACTED]
140.	08/10/2019	QWL.PLCMNT.ASX	AW	\$30,000	[REDACTED]

**Confidential Annexure A: Bulk Transacting Fraud Monitoring Rules**



