Federal Court of Australia
District Registry: Victoria
Division: General

AUSTRALIAN PRUDENTIAL REGULATION AUTHORITY

Applicant

BENDIGO AND ADELAIDE BANK LIMITED (ACN 068 049 178)

Respondent

STATEMENT OF AGREED FACTS AND ADMISSIONS

A. INTRODUCTION

1. This Statement of Agreed Facts and Admissions is made jointly by the Applicant (**APRA**) and the Respondent (**BEN**) pursuant to s 191 of the *Evidence Act 1995* (Cth), in relation to proceedings commenced by APRA against BEN on 10 August 2026 (**Proceeding**).

2. This document contains facts relevant to each of the contraventions alleged by APRA and admitted by BEN for the purpose of the Proceeding. The facts, and the admissions, are agreed to and made solely for the purpose of the Proceeding and do not constitute any admission outside of the Proceeding.

3. Unless otherwise stated, the facts and admissions made in this Statement relate to the period between 2 June 2020 and 1 July 2023 (**relevant period**).

B. PARTIES

B.1. Australian Prudential Regulation Authority

4. APRA is the Australian Prudential Regulation Authority established under s 7 of the *Australian Prudential Regulation Authority Act* 1998 (Cth) (**the APRA Act**).

Filed on behalf of (name & role of party) Australian Prudential Regulation Authority, the Applicant
Prepared by (name of person/lawyer) Alana Giles
Law firm (if applicable) Holding Redlich
Tel +61 3 9321 9996 Fax (03) 9321 9900
Email Alana.Giles@holdingredlich.com
Address for service (include state and postcode) Level 23 500 Bourke Street Melbourne VIC 3000

5. The main purposes for which APRA exists are set out in s 8 of the APRA Act and include regulating bodies in the financial sector in accordance with other laws of the Commonwealth that provide for prudential regulation. APRA has the functions conferred on it by the APRA Act and also those functions conferred on it under the *Banking Act 1959* (Cth) (**Banking Act**).

6. Pursuant to s 13(1)(a) of the APRA Act, APRA is a body corporate with perpetual succession and it may sue and be sued pursuant to s 13(1)(c) of the APRA Act.

B.2. Bendigo and Adelaide Bank Limited

7. BEN is:

   (a) a corporation incorporated under the *Corporations Act 2001* (Cth) and able to be sued in its own name; and

   (b) an authorised deposit taking institution (**ADI**) within the meaning of s 5 of the Banking Act which was granted an authority to carry on a banking business on 29 June 1995.

8. During the relevant period, BEN operated the Alliance Bank, a network of five authorised representatives operating under BEN's ADI (as described in paragraphs 44, 45 and 48 below).

C. BEN'S POLICY FRAMEWORK FOR INFORMATION SECURITY

9. During the relevant period, BEN maintained the following policies applicable to information security, including customer authentication controls for access to the Alliance Bank's mobile and internet banking platforms:

   (a) Information Security Policy;

   (b) Group Operations Risk Management Framework (**Operational Risk Framework**), which included at Annexure A, an Escalation Matrix;

   (c) Password Management Standard;

   (d) Group Technology Risk Management Framework (**TRMF**);

   (e) Controls Testing Framework (**CPS 234 Framework**);

   (f) Business System Ownership Policy;

(g) Control Standard; and

(h) Cyber Incident Response and Major Incident Plans.

C.1. Information Security Policy

10. The Information Security Policy applied to BEN, including Alliance Bank.

11. The stated purpose of BEN's Information Security Policy was to "…outline the approach for managing information security and to establish support for information security, and by extension Cyber Security to ensure the protection of [BEN]'s information, systems and technology related assets in accordance with [BEN]'s objectives and risk appetite".

12. The Information Security Policy required:

(a) Business System Owners to:

(i) ensure information security controls are implemented and maintained within the risk appetite of the Group and directly aligned to the classification of the asset, under versions 3.3 and 3.4 of the Information Security Policy;

(ii) implement and maintain information security controls based on the classification of information and technology assets and in line with the Group's security and risk management policies and standards, under version 3.5 Information Security Policy;

(b) information security controls to be tested throughout the Group on a rolling program based upon risk profile; and

(c) from version 3.5 (applicable from July 2022), key information security controls to be tested periodically using a rolling program based upon risk profile and business value.

13. The Information Security Policy set out a 'three lines of defence' system as follows:

(a) the first line of defence required that:

(i) applicable policies, procedures and guidelines were followed by all staff in their day-to-day operations;

(ii) information security incidents were reported in accordance with the incident management policy and processes;

(iii) all employees had a practical understanding of the Information Security Policy as relevant to their role;

(iv) each individual executive and business unit head had day to day responsibility and accountability for the management of information security in their business;

(v) executive and business unit heads understood and managed the risks associated with the systems and information required for the successful execution of their processes and achievement of their business objectives;

(b) the second line of defence required:

(i) risk specialists or Business Unit Risk Advisors to ensure information security risks were identified, reported and rated through approved processes, and ensure information security risks and associated controls were recorded and monitored within BEN's operational risk management system called CURA (**CURA**);

(ii) technology and data risk, and group operational risk, provided independent advice, challenged and oversaw activities within their business unit or division that may have associated operational risks, including information security risks, as a second line of defence; and

(c) the third line of defence was Group Internal Audit, which would provide independent assurance reviews of the adequacy and effectiveness of first and second line compliance and operational effectiveness of the Operational Risk Framework.

14. From 1 July 2022, the Information Security Policy was amended to require that:

(a) periodic testing be conducted based upon risk profile and business value in line with the CPS 234 Framework; and

(b) Information Security controls operated by service providers must be actively monitored and managed using a risk-based approach.

C.2. Operational Risk Framework

15. The Operational Risk Framework applied to BEN, including Alliance Bank.

16. The stated purpose of the Operational Risk Framework was to detail, in combination with several other risk management frameworks, BEN's approach for each of its material risks.

17. An aspect of BEN's approach for assessing its material risks was an annual risk and control self-assessment (**RCSA**). The RCSA assessed, among a range of risks, the information security and cyber security risks associated with BEN's information systems, hosted both internally and on behalf of BEN by third parties.

18. The Operational Risk Framework required that all identified operational risks that were above the threshold set in BEN's Risk Rating Matrix were to be included in the applicable Risk Register within CURA. CURA was used for recording and monitoring (via notifications) BEN's risk profile at a Business Unit, Divisional and Group level through the use of a dashboard.

19. The Operational Risk Framework required BEN to identify, assess, treat, monitor and report on its operational risks, including its information security risks, consistently across the Group. Each identified operational risk was to be assessed on an inherent and residual basis, and rated by reference to BEN's Consequence Table and Risk Rating Matrix.

20. The Operational Risk Framework contained an Escalation Matrix which together with the related Escalation Matrix Processes set out how identified risk events were to be treated and escalated within BEN.

21. **Password Management Standard**

22. The Password Management Standard was approved by BEN's Technology Risk Committee (**Technology Risk Committee**) on 8 March 2022 and applied to BEN, including Alliance Bank, from 1 July 2022.

23. The Password Management Standard required, amongst others, the following minimum requirements:

    (a) For customer application passwords, a minimum password length of 8 characters for "Low/Medium Risk Applications" and for "High Risk Applications" including for systems managed or hosted by a third-party service provider on behalf of BEN, customer passwords were required to have a minimum length of 8 characters, multi-factor authentication and any 3 of uppercase, lowercase, numbers or special symbols characters;

    (b) Newly set passwords must prevent the use of sequential characters, i.e., "1234567", "abcdefg"; and

    (c) New and reset passwords set on behalf of users must be sufficiently randomised to minimise the likelihood of compromise of unused accounts.

C.3. BEN's Technology Risk Management Framework

24. The TRMF applied to BEN, including Alliance Bank, during the relevant period.

25. The TRMF sat under the Operational Risk Framework. The TRMF set out a description of the risk management strategy for BEN and its controlled entities. "Technology Risk" fell within the scope of "Operational Risk" and was defined by BEN within the TRMF as the "governance, people, process or technology risks which result in loss or negative impact to … the Group's IT environment or parts of the IT environment, including infrastructure, systems, applications and data".

    (a) The TRMF set out a 'three lines of defence' system consistent with that described in the Information Security Policy described at paragraph 13 above. The first line of defence required individual business units to identify technology risks within the business unit, design and implement controls to mitigate technology risks, process execution and effectively perform control procedures. BEN's Technology & Transformation function was responsible for designing and implementing controls to mitigate technology risks. The Technology & Transformation function was supplemented by a Technology & Transformation Risk function which was responsible for proactively managing operational and technology related risks and conducting risk assessments.

    (b) The second line of defence required the independent Technology and Data Risk function within BEN's Operational Risk to be responsible for the establishment and implementation of the framework, governance and structures for technology risk management, providing independent and objective oversight, advice and influence to Line 1, and reporting and escalating technology related risks and defining the suite of risk metrics and risk indicators.

    (c) The third line of defence was BEN's Group Internal Audit which was to provide independent assurance and oversight to ensure BEN's framework of risk management, control, and governance processes were adequate and functioned effectively.

26. For the purposes of the Banking Executive Accountability Regime (formerly at Part IIAA of the Banking Act) (**BEAR**) accountability, the TRMF set out that accountable persons were responsible for the aspects related to technology risk management that were under their control, with those accountable persons required to take reasonable steps to ensure that the activities outlined in the TRMF were followed. The TRMF stated the Chief Transformation Officer (**CTO**) of BEN had been assigned as the BEAR Accountable Executive for information security, cyber security and data protection.

27. Under the TRMF, information security control design assessments for third parties who managed BEN information assets were to be performed by the Information Security Practice within BEN's Technology and Transformation team. The Information Security Practice was responsible for, among other matters, designing, implementing, and operating mechanisms to detect and respond to information security incidents, and testing BEN's information security response plans at least annually.

C.4. BEN CPS 234 Controls Testing Framework

28. On or about 30 June 2020, APRA approved an adjustment to CPS 234 Information Security (**CPS 234**) for BEN, such that the date by which CPS 234 was to apply to information assets managed by a third party was extended to 1 January 2021.

29. The CPS 234 Framework applied to BEN, including Alliance Bank, from 30 September 2020.

30. The stated purpose of the CPS 234 Framework was to guide BEN on controls testing activities to ensure compliance with CPS 234. The CPS 234 Framework was intended to provide a link between CPS 234 and the Operational Risk Framework, and sat under the TRMF.

31. The CPS 234 Framework provided guidance on:

    (a) identifying the totality of the information security controls that BEN was responsible for and reviewing it for completeness against CPS 234 (**CPS 234 Controls Universe**);

    (b) control design documentation and assessment;

    (c) assurance mapping to ensure completeness of the systematic testing program, and identify the business unit accountable for testing of information security controls within the bank and to identify key gaps in testing and key applications to be tested;

    (d) a systematic controls testing program, including detailed design of controls assessment, security testing of controls, and control validation testing and effectiveness;

    (e) monitoring of control weaknesses and remediation; and

    (f) reporting of control weaknesses to APRA.

32. BEN used the National Institute of Standards and Technology Cyber Security Framework as a starting point for the CPS 234 Controls Universe. The CPS 234 Framework also provided that

information security controls would be specific for each individual application, including the application for password configuration.

33. The CPS 234 Framework provided that control testing to meet the requirements of CPS 234 was to include various techniques using both controls validation (audit style) and security controls testing. Examples of security controls testing included penetration testing and vulnerability scanning. Such testing was to be performed by staff with appropriate skills and was to be functionally independent. Security penetration testing was to be performed by independent resources or staff that do not have accountability for the controls being tested. Password configuration was identified as a type of control.

34. The CPS 234 Framework provided that it was the role of an executive or business unit head to ensure that appropriate assurance activities had been completed.

35. From 24 March 2021, the CPS 234 Framework was amended to additionally require control design weaknesses to be recorded as risk treatments in CURA and for the Technology Risk Team to perform control validation, record control effectiveness in CURA and report results to the Technology Risk Committee.

C.5. BEN Business System Ownership Policy

36. The Business System Ownership Policy applied to BEN, including Alliance Bank, during the relevant period.

37. The stated purpose of the Business System Ownership Policy was to provide a structured and consistent approach for business system ownership within BEN.

38. Under the Business System Ownership Policy, the Business System Owner (**BSO**) was responsible for:

    (a) ensuring business systems functionality met the needs of their business unit;

    (b) maintaining visibility of and ensuring funding is available for the entire business system lifecycle;

    (c) providing direction and approving decisions of changes to required business systems; and

    (d) liaising with Domain Leads to ensure business systems are kept current.

39. From 24 May 2022, the Business System Ownership Policy was amended to provide that the BSO was also responsible for:

    (a) identifying, assessing, measuring, recording and reporting on risks related to the business systems and escalating in accordance with the Operational Risk Framework; and

    (b) escalating issues to BEAR accountable executives where required; for example, if a failure to remediate an application issue would result in non-compliance with legislation it was required to be escalated to the relevant BEAR accountable executive.

40. From 24 May 2022, the Business System Ownership Policy also set out the role of the "TnT Service Owner" who was accountable for, amongst other matters:

    (a) ensuring that a BSO is identified for all relevant business systems within BEN;

    (b) ensuring that business systems and supporting infrastructure relevant to their service are fit for purpose to support the business capabilities aligned with the needs expressed by the BSO;

    (c) incident management; and

    (d) escalating issues to the BEAR accountable executive where required, for example, if failure to remediate an application issue will result in a high residual information security risk it must be escalated to the technology BEAR accountable executive in accordance with the Operational Risk Framework.

C.6. BEN Control Standard

41. From at least August 2022, the Control Standard applied to BEN, including Alliance Bank.

42. The purpose of the Control Standard was to set the minimum requirements and standards for control management within BEN.

43. From December 2022, the Control Standard was amended to set out the additional requirements on Technology controls (including information security controls) to ensure compliance with CPS 234, including:

    (a) controls validation testing to be performed by independent resources/staff with appropriate IT controls experience;

(b) security penetration testing to be performed by independent resources/staff that do not have accountability for the controls being tested (e.g. firewall configuration);

(c) that the sufficiency of the testing program must be reviewed at least annually or when there is a material change to the information assets or the business environment;

(d) information security control weaknesses were to be considered under the Operational Risk Framework, particularly where they relate to key controls which are required to be reflected in CURA with the associated treatment plans;

(e) assessment of information security material control weaknesses;

(f) monitoring of information security material control weaknesses;

(g) considering whether notification to APRA of material control weaknesses is required;

(h) the BSO was responsible for application-level technology controls in accordance with the Business System Owner Policy; and

(i) the BSO was responsible for application controls in accordance with the Business System Owner Policy.

D. ALLIANCE BANK

D.1. Transfer of business of Alliance Partners to BEN

44. In December 2014, BEN entered into an agreement (**Alliance Agreement**) to launch a new banking model called Alliance Bank, with the following entities:

(a) AWA Mutual Limited (ACN 087 651 652) (**AWA**);

(b) BDCU Limited (ACN 087 649 787) (**BDCU**);

(c) Circle Mutual Limited (ACN 087 650 968) (**Circle**); and

(d) Service One Mutual Limited (ACN 095 848 598) (**Service One**),

(together, the **Alliance Partners**).

45. The Alliance Partners were former credit unions that surrendered that status upon joining the Alliance Bank model, instead becoming authorised representatives of BEN.

46. On 1 March 2015, APRA issued certificates of transfer under s 18 of the *Financial Sector (Business Transfer and Group Restructure) Act 1999* (Cth) in respect of the partial transfer of business by each of the Alliance Partners to BEN, and those certificates came into force on that date.

47. Under the terms of the Alliance Agreement, the Alliance Partners and BEN agreed that customer information data for each Alliance partner would be migrated to BEN's core banking system. The Alliance Agreement contemplated that the migration would be completed within 2 years.

48. On 4 May 2018, Nova Mutual Limited (ACN 087 650 440) (**Nova**) became one of the Alliance Partners on substantially the same terms as the Alliance Agreement, and APRA issued a certificate of transfer under section 18 of the *Financial Sector (Business Transfer and Group Restructure) Act 1999* (Cth) in respect of Nova.

49. As a result of the Alliance Agreement and transfers identified in paragraphs 46 and 48 above, Alliance Bank customers became customers of BEN.

50. As at July 2020, Alliance Bank had approximately 38,000 customers (out of approximately 1.88 million customers of BEN).

D.2. Products and services offered by Alliance Bank to customers

51. During the relevant period, Alliance Bank offered its customers banking products and services including complete access debit accounts, at call and term deposit accounts, credit cards, and loan accounts.

52. During the relevant period, customers of Alliance Bank were offered functionality to access their accounts online, including to make and receive payments through:

    (a) online banking through an Internet browser on a computer or other non-mobile device (**Online Banking**);

    (b) online banking through an Internet browser on a mobile device (**Mobile Banking**); and

    (c) mobile banking through a mobile banking application accessed through a mobile device (**Mobile App**),

    (together, **Digital Access**).

D.3. Core banking platform used by Alliance Bank during the relevant period

53. Prior to the establishment of the Alliance Bank, each of the Alliance Partners operated their banking functions using software called Ultracs. Ultracs was a core banking system software provided and supported by Ultradata Australia Pty Ltd (**Ultradata**).

54. Upon the establishment of the Alliance Bank, all service agreements between the Alliance Partners and third-party service providers, including Ultradata, were effectively novated to BEN by virtue of the certificates of transfer referred to in paragraphs 46 and 48 above.

55. On or about 1 November 2016, BEN entered into a Software Licence and Maintenance Agreement with Ultradata for the provision of Ultracs to the Alliance Partners (**SLAM Agreement**).

56. On or about 18 February 2022, BEN and Ultradata entered into a Deed of Variation of the SLAM Agreement (**Deed of Variation**) pursuant to which the term of the SLAM Agreement was extended for a further period of three years to 18 February 2025.

57. Under the SLAM Agreement:

    (a) Ultradata granted BEN a non-exclusive licence to use Ultracs and agreed to provide second line maintenance services in respect of that software;

    (b) Ultradata agreed that BEN could grant a right to the Alliance Bank to use Ultracs, provided that any use by an Alliance Partner would be deemed to be use by BEN; and

    (c) the separate software licence agreements that had previously existed between each of the Alliance Partners and Ultradata terminated, with the Alliance Bank thereafter permitted to use Ultracs in accordance with the terms of the SLAM Agreement.

58. Alliance Bank operated on four different instances of Ultracs, each providing Digital Access with similar, though not identical, customer access control configurations.

59. The instances of Ultracs were for:

    (a) AWA Alliance Bank;

    (b) BDCU Alliance Bank;

    (c) Circle Alliance Bank; and

    (d) Service One Alliance Bank and Nova Alliance Bank.

D.4. Managed services for Alliance Bank core banking platform during the relevant period

60. Ultracs for each of the Alliance Partners was hosted by TransAction Solutions Limited (ACN 084 571 040), trading as TAS, which was rebranded in 2022 as Experteq (**TAS**).

61. Service agreements between the Alliance Partners and TAS were effectively novated to BEN by virtue of the certificates of transfer referred to in paragraphs 46 and 48 above.

62. On or about 12 October 2016, BEN entered into a managed services agreement with TAS for the provision by TAS of services and infrastructure, including in respect of the Ultracs core banking system for the Alliance Partners for a period of five years (**TAS Agreement**).

63. On 5 September 2017, BEN entered into a Fraud Management Services Agreement with Cuscal Limited (ACN 087 822 455) (**Cuscal**) pursuant to which Cuscal agreed to provide managed fraud monitoring and detection services known as "Vigil Services" in respect of card-based transactions for the Alliance Partners.

64. On or about 4 June 2018, BEN entered into Extended Fraud Management Services Agreements with Cuscal pursuant to which Cuscal agreed to provide Vigil Services for New Payments Platform (**NPP**) transactions (including OSKO payments) and monitoring of associated PayID activity in respect of each of the Alliance Partners.

65. In or about September 2018, BEN introduced real-time send or receive functionality of payments using the NPP in relation to customers of Alliance Bank across all of the banking facilities.

66. On or about 12 October 2021, BEN entered into a further managed services agreement with TAS for the provision by TAS of services and infrastructure including in respect of the core banking system for the Alliance Bank.

67. The Ultracs system used by Alliance Bank was not used by any other part of the Group, nor did the relationship with TAS and Ultradata extend beyond Alliance Bank.

68. By no later than 9 December 2021, BEN determined the Ultracs system was a critical and sensitive information technology asset of BEN.

69. From 1 January 2021 to the end of the relevant period, the information assets of BEN for the purposes of CPS 234 (defined in CPS 234 as information and information technology, including software, hardware and data (both soft and hard copy)), included:

(a) the Ultracs core banking software used to process Alliance Bank customer accounts and transactions;

(b) the software comprising the Online Banking internet portal and the Mobile Banking application through which customers of Alliance Bank accessed their accounts;

(c) the hardware and hosting infrastructure operated by TAS/Experteq on which those systems operated; and

(d) the customer data held within those systems, including Alliance Bank customer account credentials and transaction records.

D.5. Use of business managed information technology services for Alliance Bank by BEN and BEN's responsibility for the Alliance Bank information security controls

70. Ultracs and the TAS services used by Alliance Bank were managed and operated by the Alliance Bank business unit as "business managed IT" (**BMIT**). Under the BMIT model, the business unit using a third-party technology service had primary responsibility for managing that service, with support from the Technology & Transformation Division. BEN remained ultimately responsible for the information security controls in place for Alliance Bank, including for Digital Access.

71. The Ultracs system was separate to BEN's core banking system, RFS-B (**RFS-B**), which was used for internet and mobile banking by most BEN customers. BEN's RFS-B system was managed by the Technology & Transformation division within BEN that reported to the Chief Transformation Officer, the Chief Information Officer and the Chief Information Security Officer.

72. From at least 25 June 2020 to 7 December 2022, concerns about BMIT were raised at BEN committee and Board level meetings, including that:

(a) all technology should be managed by BEN's Technology & Transformation division, with any exceptions to be determined on a case-by-case basis, and with BEAR responsibility assigned to the relevant business executive;

(b) BMIT was introducing a risk that BEN did not know all technology being used across the organisation, which could lead to unidentified vulnerabilities existing;

(c) there remained some BMIT systems which posed an ongoing risk, and an action item was created to identify the residual BMIT systems involving customer data to identify risks and prioritise any with customer data; and

(d) the ongoing existence of BMIT and the reason why it was taking a significant amount of time to action an agreed position was queried.

D.6. Decision to migrate Alliance Bank from Ultracs to RFS-B

73. Throughout 2020 and 2021, Executive Committee meetings noted recommendations that BEN exit the Alliance Bank model and migrate customers of Alliance Bank to RFS-B. In particular:

(a) On 5 August 2020, an Executive Committee paper meeting detailed initial target dates of commencing the migration in September 2020, with an ideal end date being February 2022 and critical end date being April 2022. Business risks were acknowledged in not migrating, including that the Alliance Partners had significantly reduced staff with system knowledge and project experience and in the past two years they had advised that they had insufficient resources to test and implement changes to processes and systems.

(b) On 20 October 2020, a further Executive Committee paper was prepared which noted that there would be challenges to exiting the Alliance Bank model before March 2025, as this would be a breach of franchise agreements with the Alliance Partners. It also noted that a decision to delay migration would prevent the business from leveraging the scale of the Group and result in $5.1m per annum of vendor costs.

(c) By 16 December 2020, BEN had decided it would seek to progressively migrate customers of Alliance Bank to BEN's core banking system, RFS-B, however this remained subject to negotiating changes to the franchise agreements with the Alliance Partners. BEN began planning for a migration of the Alliance Partners into the BEN core RFS-B banking system, subject to the decision of each Alliance Partner agreeing to migrate or exit.

74. By September 2021, BDCU Alliance Bank had agreed to migrate within BEN with a timeframe set to be finalised by September 2022. The other Alliance Partner migrations were expected to be completed progressively by September 2023.

75. By 5 March 2023, BDCU was migrated to BEN's core banking system, and Service One, Nova and Circle were migrated by the end of June 2023. By March 2025, AWA exited BEN.

E. RISK OF UNAUTHORISED ACCESS AND UNAUTHORISED PAYMENTS

76. During the relevant period, the risk of unauthorised third-party access to customer accounts was known to BEN. This included the possibility of third-party access to customer accounts to make unauthorised payments between and out of customer accounts. A common method during the

relevant period for gaining unauthorised access to customer accounts was known to be cyber-attacks, including "brute force attacks."

77. In particular, BEN's November 2022 Cyber Security Update to the BEN Board:

(a) referred to then recent high profile cyber incidents in Australia, including Optus and Medibank, and several other Australian organisations that had been impacted by cyber threats, including the Australian government;

(b) stated that Australian organisations were increasingly being targeted by both sophisticated cyber-criminal organisations and opportunistic, less sophisticated cyber threat actors;

(c) stated that BEN operated in a significantly heightened and changing cyber threat landscape, and that Australian regional banks are facing increasing cyber threat risk; and

(d) identified recent cyber activity, including recent brute force attacks on BEN and identified that sometime after 30 September 2022, brute force attacks were also experienced by Alliance Bank, specifically targeting BDCU and Service One.

F. ALLIANCE BANK BUSINESS UNIT

F.1. The Alliance Bank business unit

78. Under the BMIT model, Business System Owner Policy and Information Security Policy, the person responsible for information security for Alliance Bank and the BSO for Ultracs during the relevant period was the Head of Alliance Bank.

79. During the relevant period, the Head of Alliance Bank:

(a) was not an accountable person of BEN within the meaning of the BEAR;

(b) was identified in BEN's enterprise risk management system, CURA, as the risk owner for the following Alliance Bank risks:

(i) External Fraud, being the risk of external theft and fraud being perpetrated by external parties (customer or third party), caused by, amongst other things, hacking of the Internet Banking platform, identity takeover (including customer emails) and unauthorised transactions to customer accounts; and

(ii) Breach of IT Security, being the risk of an external hacker breaching security and stealing customer information including card details, disrupting the infrastructure or attempting to process fraudulent transactions,

(together, the **Alliance IT Risks**); and

(c) did not have any professional background or formal qualifications in information technology or information security.

G. BEN DID NOT HAVE ADEQUATE CUSTOMER AUTHENTICATION CONTROLS FOR ALLIANCE BANK

G.1. Alliance Bank Password settings

80. In the context of CPS 234, customer authentication controls include controls for:

(a) the identification and verification of a customer;

(b) the protection of sensitive and confidential data;

(c) the prevention of unauthorised access to systems and data; and

(d) monitoring of potential illicit activity from threat actors,

(**customer authentication controls**).

81. During the relevant period prior to 27 March 2023 (or in the case of BDCU, prior to its migration to BEN's RFS-B System on 3 March 2023), the customer authentication controls for Alliance Bank included the following characteristics:

(a) For Service One, Nova and BDCU Alliance Banks:

(i) the minimum requirement for passwords was six characters with a minimum of one number;

(ii) it was possible for a user to set an insecure password known to be vulnerable and compromised, such as "password1" or "123456";

(b) for AWA and Circle Alliance Banks:

(i) the minimum password length was four characters;

(ii) the use of default passwords resulted in AWA's most common password being "1234"; and

(iii) numerous Circle customers still had passwords allocated by Circle in 2008 and 2012.

82. During the relevant period, the password controls in place for customers on BEN's RFS-B system were as follows:

(a) the minimum password length was eight characters;

(b) all passwords were required to contain at least one alpha character, one numeric character, no spaces and special characters were permitted;

(c) after 360 days of inactivity, BEN's customers could not login using their existing password and were required to reset their password;

(d) password history was set to one to prevent customers from reusing previous passwords used; and

(e) mandatory Multi Factor Authentication was imposed on customer accounts through use of a security token from 1 July 2019 and One-time passwords via SMS or email from 22 February 2022.

G.2. BEN's knowledge of and response to customer authentication control issues

83. In or around September 2017, BEN's Information Security team engaged Deloitte to conduct a review on technology risks and controls specifically in relation to the services provided by Ultradata and Experteq (**Deloitte Report**). The Deloitte Report observed that:

(a) information security governance at Ultradata appeared immature;

(b) there was an absence of regular independent information security assessments for the Ultradata environment; and

(c) BEN should perform regular application penetration testing over the Ultracs application and related internet banking modules.

84. The findings of the Deloitte Report were shared with Ultradata and a treatment plan was jointly developed for the resolution of control gaps identified and for the overall improvement in risk management and control practices.

85. Further to the Deloitte Report, in August 2018, BEN conducted a "Third Party IT Controls Review" for Alliance Bank in relation to each of Ultradata and TAS that was provided to the Head of Alliance Bank and highlighted the need to perform regular application penetration testing over Ultracs.

86. On 17 October 2019, BEN's Board Technology Committee, which was responsible amongst other things for overseeing the delivery of technology operations for BEN, was informed that a high priority recommendation remained open for penetration testing of the Ultracs application and external testing was expected by 4 November 2019. The external testing was not conducted until approximately May or June 2020. The relevant paper presented to BEN's Board Technology Committee noted that BEN's Information Security team had, as of July 2019, reviewed security testing provided by Ultradata and that "[a]lthough no outstanding concerns were noted with respect to independent security assessments Information Security determined that further specific testing should be undertaken".

87. In May 2020, BEN finalised arrangements for CQR Consulting Australia Pty Ltd (**CQR**, now known as **CyberCX**) to conduct penetration testing of the Service One instance of Ultracs. On or about 2 June 2020, CQR provided a report to BEN's Information Security team of the penetration testing it had undertaken of the customer authentication controls on the Ultracs instance used by Service One Alliance Bank (**Penetration Test Report**).

88. The Penetration Test Report findings included that:

(a) when setting a member's password in the application, there were insufficient complexity requirements and it was possible to set an easily guessed password, such as "password1"; and

(b) weak password policies would make it easier for attackers to brute force user passwords, which if successful would allow access to that user's account.

89. CQR recommended that Service One implement password complexity requirements when a user set their password which aligned with security best practice, being passwords of a minimum length of eight characters (12 preferred), minimum one uppercase character, one lowercase character, one number and one symbol.

90. The Penetration Test Report also identified that:

(a) member numbers could be identified by iterating through potential member numbers and reviewing the type of error message that was reported by the application. If the attacker's

program guessed a valid member number, the Ultracs instance used by Service One would return a different error message from the application; and

(b) coupled with weak passwords, an attacker would be able to easily iterate through member numbers and perform password spray attacks, increasing the likelihood of account compromise.

91. CQR rated each of the findings in paragraphs 88 and 90 (together, the **Vulnerability Findings**) as presenting a 'moderate' risk. It recommended that a change be made to the Ultracs login portal to show the same message regardless of whether a valid member was entered or not.

92. The Penetration Test Report also identified the following controls that were not in place for the Service One Alliance Bank instance of Ultracs:

(a) the application had not implemented CAPTCHA (Completely Automated Public Turing Test to tell Computers and Humans Apart, **CAPTCHA**); and

(b) that while the Service One instance supported SMS authentication "One Time Password" multi-factor authentication (**OTP**), the use of OTP was optional and Service One Alliance Bank customers had to choose to apply it.

93. The findings of the Penetration Test Report were:

(a) reviewed and logged by a member of BEN's Technology division into Nucleus, a vulnerability aggregating tool used by BEN's Information Security team to record penetration test findings and track vulnerabilities identified; and

(b) not provided to TAS, despite a suggestion by BEN's Technology Division they be provided to TAS for TAS to take action in respect of the findings.

94. These 'moderate' rated findings were not further escalated to BEN or Alliance Bank management, nor were the findings considered or assessed against BEN's Operational Risk Framework Escalation Matrix. In particular, the Penetration Test Report was not provided to the Head of Alliance Bank as the BSO for Ultracs and the risk owner of the Alliance IT Risks, and the vulnerabilities identified were not remediated until March 2023.

95. No further testing of a kind similar to the Penetration Test Report was prepared for BDCU, Nova, Circle or AWA within Alliance Bank prior to March 2023.

G.3. October 2022 Attacks on Alliance Bank

96. On or about 27 October 2022, a threat actor conducted brute force login attacks on the Ultracs instances of BDCU Alliance Bank and Service One Alliance Bank (**October 2022 Attacks**).

97. The October 2022 Attacks attempted to exploit the same customer authentication control deficiencies for Digital Access for Alliance Bank that had been identified in the Penetration Test Report in June 2020.

98. None of the accounts of customers of BDCU Alliance Bank and Service One Alliance Bank were accessed by the threat actor. Thousands of customers of BDCU Alliance Bank and Service One Alliance Bank were automatically locked out of their account when the threat actor made three unsuccessful attempts to access each account.

99. Neither BEN nor its service providers monitored suspicious or increased login activity to the accounts of Alliance Bank customers (but did monitor accounts for suspicious transactions) and the October 2022 Attacks were detected as a result of Alliance Bank Customers contacting BDCU to report that their internet banking access had been locked.

100. In October 2022, Experteq (formerly TAS) recommended to the Head of Alliance Bank following the October 2022 Attacks, that Alliance Bank should consider implementing the following controls:

(a) migrating members to non-numeric IDs as soon as possible;

(b) increasing minimum password lengths;

(c) Multi Factor Authentication to member accounts; and

(d) CAPTCHA to logins in order to defeat automated connections.

101. Experteq also advised the Head of Alliance Bank that the October 2022 Attacks appeared to have been focused on banks that still have accounts with numeric ID's which could allow a threat actor to iterate through [customer number] ID's sequentially.

102. Following and in response to the October 2022 Attacks, BEN implemented a Cloudflare Web Application Firewall (**WAF**) and a CAPTCHA solution for each of the instances of Ultracs used by Alliance Bank for Online Banking.

103. At that time, CAPTCHA was inadvertently not implemented for Mobile Banking.

104. The October 2022 Attacks constituted a material change to the business environment for Alliance Bank within the meaning of paragraph 27(c) of CPS 234.

105. On 31 October 2022, BEN submitted a CPS 234 Incident Notification to APRA stating among other matters that:

(a) several brute force attacks had been initiated against BDCU, in addition to one attack on Service One;

(b) accounts targeted by the attack were automatically locked after three failed attempts;

(c) BEN had geo-blocked the relevant IP addresses involved in the attack;

(d) WAF protection had been applied by TAS for BDCU and was being rolled out across all five Alliance Bank Partners in the wake of the attacks; and

(e) BEN were exploring other mitigating controls to manage ongoing threats.

106. On 25 November 2022, the Head of Alliance Bank received a bulk email entitled "Envisage Extra – Ultradata not compromised by Brute Force Attacks" (**Envisage Email**). The Envisage Email, which was an email in the nature of an information update sent to Ultradata's clients, and not specifically addressed to the Head of Alliance Bank, advised that Ultracs had not been compromised by the attacks. Ultradata then recommended that Ultracs users consult their host organisation to consider appropriate options offered within Ultracs to prevent brute force attacks, including:

(a) two-factor authentication for user login;

(b) using CAPTCHA (to prevent automated brute force attacks);

(c) enforcing strong passwords for clients; and

(d) requiring settings that will mitigate the impact of account compromise, including requiring two-factor authentication for new payees and setting payment limits for accounts.

107. On 29 November 2022, Experteq issued an Information Security Note to its clients, including BEN, regarding internet banking brute force attacks, which recommended the implementation of Multi-Factor Authentication at login, CAPTCHA as part of the login process, measures to ensure that authentication failures for invalid member numbers produced the same result as failures for incorrect passwords, increasing minimum password length and complexity requirements,

disallowing common passwords, and avoiding contiguous member numbers and using member numbers as usernames.

108. On 29 November 2022, a cyber security update to the BEN Board noted the October 2022 Attacks and that BEN was at a critical point of needing further investment in resourcing and capability to increase confidence in its ability to protect and defend its organisation against security attacks.

109. BEN did not subsequently undertake a substantive review of the October 2022 Attacks nor undertake a review of the customer authentication controls that were in place for Digital Access for Alliance Bank.

110. The recommendations of Experteq and Ultradata identified in paragraphs 100, 106 and 107 above were not implemented by BEN prior to March 2023, save insofar as BEN, in November 2022, implemented a CAPTCHA solution for each instance of Ultracs used by Alliance Bank for Online Banking (but not Mobile Banking) as referred to in paragraphs 102 and 103 above.

G.4. Inadequate customer authentication controls for Alliance Bank

111. During the relevant period, BEN did not have in place adequate customer authentication controls for the prevention and detection of unauthorised access and unauthorised payments for Alliance Bank Customers, in that BEN did not:

(a) prior to March 2023, implement mandatory password complexity requirements (such as the minimum password length of eight characters, the use of letters or special characters or a password expiry) as required by BEN's Password Management Standard;

(b) prior to March 2023, disallow the use of common passwords for Alliance Bank, such as by requiring each customer with a common password to reset to a more complex password before they could use online banking;

(c) prior to March 2023, implement mandatory Multi-Factor Authentication or SMS OTP to authenticate Alliance Bank member access to the Online Banking login portal or payment to a “new Payee”, which were available to Service One and BDCU to implement, and which had been implemented in various optional forms prior to the relevant period;

(d) prior to November 2022 for AWA, Circle and Service One, BDCU and Nova Alliance Banks, have in place adequate human verification or anti-automation controls (such as, CAPTCHA) across Online Banking;

(e) prior to March 2023, have in place adequate human verification or anti-automation controls (such as, CAPTCHA) for Mobile Banking; and

(f) have in place adequate controls to prevent Alliance Bank customer member numbers to be ascertainable in the Online Banking login portal for Ultracs, by reason of different error messages for valid and invalid member numbers, that enabled an attacker to identify Alliance Bank customer accounts to target.

H. BEN DID NOT HAVE IN PLACE A SYSTEMATIC TESTING PROGRAM OF CUSTOMER AUTHENTICATION CONTROLS FOR ALLIANCE BANK

112. From 30 September 2020 to 1 July 2023, when BEN had in force the CPS 234 Controls Testing Framework, BEN did not have in place a systematic testing program for the customer authentication controls applicable to Alliance Bank.

H.1. Reliance on Alliance Bank Business Unit for testing of customer authentication controls

113. BEN's Alliance Bank business unit was responsible for setting the controls for Digital Access for Alliance Bank and testing the adequacy of those controls, and conducted annual control testing of its information security controls. Other than the Penetration Test Report, the Alliance Bank business unit's annual control testing program did not include testing of customer authentication controls for Alliance Bank.

114. BEN's Technology and Transformation team also conducted testing of Alliance Bank controls, including procuring the penetration test of Service One's Ultracs instance in May or June 2020, leading to the Penetration Test Report being provided to BEN. BEN's Technology and Transformation team did not otherwise conduct control testing of customer authentication controls for Alliance Bank.

115. BEN configured detective controls, including relating to fraud rules and transaction monitoring, as set out at paragraphs 63 and 64 above. Experteq conducted infrastructure-level monitoring such as restricting and monitoring network traffic through firewall management and access logging.

116. During the relevant period, BEN received annual Standard on Assurance Engagements (**ASAE**) 3402 reports from TAS as to its managed operations infrastructure, which did not consider individual applications hosted on that infrastructure (**TAS Reports**). The TAS Reports did not review or assess the adequacy of customer authentication controls applicable to Digital Access for Alliance Bank.

117. In or around October 2020, BEN received an ASAE 3150 report from Ultradata which assessed the design and implementation of Ultradata's internal controls over its corporate infrastructure as at 5 October 2020. The ASAE 3150 report did not review or assess the adequacy of the customer authentication controls of the Digital Access for Alliance Bank.

118. While BEN annually reviewed the audited reports of TAS and Ultradata, these reports were not specific to the instances of Ultracs used by the Alliance Bank and did not contain any review or testing of the customer authentication controls applied within Ultracs during the relevant period across the Alliance Bank.

119. Between June and August 2022, BDO Services Pty Ltd (**BDO**) performed a control validation of Ultracs for BEN (**Ultracs Control Validation**).

120. The Ultracs Control Validation:

(a) did not review or assess the design or operating effectiveness of the customer authentication controls applicable to Digital Access for Alliance Bank; and

(b) instead, reviewed existing documentation and artefacts to identify whether there was coverage of back-end operational control areas in scope.

121. The scope of the Ultracs Control Validation did not include the customer authentication controls for Alliance Bank Online Banking or Mobile Banking.

H.2. BEN did not apply CPS 234 Controls Framework, Operational Risk Framework and TRMF to customer authentication controls for Alliance Bank

122. From 30 September 2020 to 1 July 2023, when BEN had in force the CPS 234 Framework, BEN did not apply the CPS 234 Framework to the customer authentication controls for Digital Access for Alliance Bank.

123. Between 1 January 2021 and March 2023, BEN did not perform control testing of the customer authentication controls for Digital Access for Alliance Bank, including password configuration.

124. At no time prior to the Cyber Attack did BEN:

(a) assess the Penetration Test Report and Vulnerability Findings against the CPS 234 Controls Framework, Operational Risk Framework or the TRMF;

(b) remediate the Vulnerability Findings; or

(c) escalate and report the results of the Penetration Test Report to Alliance Bank or BEN's senior management or BEN's Board.

H.3. BEN did not appropriately assess the nature and frequency of testing of the Ultracs System and TAS system

125. By March 2023, BEN had not:

(a) appropriately assessed the nature and frequency of the testing of customer authentication controls commensurate with the matters referred to in paragraph 27 of CPS 234; and/or

(b) conducted penetration testing of customer authentication controls applicable to Digital Access for Alliance Bank other than in the Penetration Test Report.

126. By reason of the matters in paragraphs 113 to 125 above, at all material times, BEN did not have in place a systematic testing program for the customer authentication controls of the Alliance Bank which were designed to test the effectiveness of Alliance Bank information security controls.

I. BEN DID NOT HAVE IN PLACE APPROPRIATE GOVERNANCE AND RISK MANAGEMENT FOR ALLIANCE BANK INFORMATION SECURITY

127. As described at paragraph 70 above, the Ultracs and the TAS services used by Alliance Bank were managed and operated by the Alliance Bank business unit as BMIT, whereby Alliance Bank had primary responsibility but relied on support and assistance from the Technology division where it lacked relevant capability.

128. The Head of Alliance Bank did not have any professional background or formal qualifications in information technology or information security. During the relevant period, Alliance Bank employed a Service Delivery Manager who reported to BEN's Technology and Transformation team and whose role was to support Alliance Bank IT infrastructure. In addition, during the relevant period, Alliance Bank was supported by BEN's Technology division as needed, as Alliance Bank's personnel had limited capability in information security. That support role was reflected in activities such as:

(a) conducting annual material information security third party assurance reviews for Ultradata;

(b) procuring the Penetration Test;

(c) co-ordinating the Ultracs Control Validation performed by BDO; and

(d) ultimately, BEN's response to the March 2023 cyber incident involving Service One, described in Section J below.

129. During the relevant period, BEN's Technology Risk Committee noted concerns about the understanding and application of risk management practices to BMIT being used across BEN (see Section D.6 above), including regarding the lack of knowledge of how Service One and the other Alliance Partners were managing risks regarding their information assets.

130. From 25 February 2021 to 1 July 2023, BEN did not have in place sufficiently clear lines of responsibility for the management of IT security for Alliance Bank. In particular, BEN did not:

(a) ensure that BEN's Technology & Transformation division had adequate operational visibility of, or oversight over, the information security controls for Ultracs, including no adequate integration of Ultracs into BEN's Security Information and Event Management system (**SIEM**) to allow BEN to monitor and detect possible notable events; and

(b) ensure that information security risks identified in the Penetration Test Report were entered into CURA and those risks were addressed or overseen by persons with relevant IT and information security experience.

J. CYBER ATTACK ON SERVICE ONE

131. On or about 3 March to 7 March 2023, an unknown person or persons (**Attacker**) conducted a brute force attack on the Ultracs instance used by Service One (**Cyber Attack**).

132. At the time that the Cyber Attack started, there were 1,598 accounts of Service One Alliance Bank customers that were protected by the password "123456". Many other accounts of Service One Alliance Bank customers were protected by other simple passwords, including "PASSWORD1", "12345678", "123456789" and "123123".

133. The number of automated attempts represented an exponential increase in traffic to Mobile Banking during that period than was ordinarily the case.

134. By this method, the Attacker accessed approximately 257 accounts of Service One Alliance Bank customers (**Accessed Accounts**), including:

(a) the Attacker accessing at least 211 of the Accessed Accounts from 3 to 5 March 2023 using the password "123456"; and

(b) the Attacker accessing at least a further 18 of the Accessed Accounts on the morning of 7 March 2023 using the password "12345678".

135. After gaining access to the Accessed Accounts, in the period from 3 March 2023 until the morning of 7 March 2023:

(a) the Attacker changed the password for at least 218 of the Accessed Accounts to a password chosen by the Attacker, being "BANNERX6", thereby preventing the relevant Service One Alliance Bank customer from accessing their account in each case;

(b) the Attacker created new payees within some of the Accessed Accounts for which OTP controls had not been activated; and

(c) the Attacker made a total of 286 transactions involving 87 of the Accessed Accounts, comprising:

(i) 66 unauthorised transfers between accounts totalling $217,190; and

(ii) 154 payments from accounts totalling $273,140.

136. In relation to the 154 payments from Accessed Accounts:

(a) 51 payments totalling $133,030 were prevented by automated fraud controls implemented by BEN from going ahead; and

(b) 103 payments totalling $140,110 went ahead and were unable to be reversed or the amounts retrieved. These funds were repaid by BEN on or about 11 March 2023 (i.e. within 4 days).

137. At about 11.12am on 7 March 2023, approximately four days after the Cyber Attack commenced, BEN became aware of the Cyber Attack following communications from a Service One member regarding fraudulent transactions.

138. BEN immediately invoked its Cyber Incident Response and Major Incident Plans. In response to the incident, BEN:

(a) shut down Digital Access for Service One Alliance customers;

(b) blocked customer account passwords that were known, or suspected, to have been compromised, and implemented further functionality to enforce complex passwords;

(c) enacted mandatory use of OTP functionality via SMS for certain internet banking transactions;

(d) restricted access to 'read-only' mode for customers who did not have OTP functionality configured;

(e) implemented geo-blocking controls limiting access to internet banking from Australian IP addresses, and blocking of suspicious or known malicious IP addresses; and

(f) increased logging and monitoring over the internet banking environment.

139. BEN's Board maintained close oversight of BEN's response to the Cyber Attack, including through regular briefings to the Managing Director, Board Chair and Board Risk Committee Chair.

140. Digital Access for Alliance Bank was placed in outage or read-only mode for Service One Alliance Bank, AWA Alliance Bank and Circle Alliance Bank customers for approximately 7 days following the Cyber Attack to allow remediation activity to be undertaken by BEN. Customers retained full access to ATM, in-branch and telephone banking facilities and continued to be able to make payments and access their cash via their cards.

141. This resulted in disruption to the online banking services provided to Alliance Bank customers and approximately 218 customer complaints being made to BEN.

K. NOTIFICATIONS LODGED WITH APRA

142. On 8 March 2023, BEN notified APRA of the Cyber Attack under paragraph 35 of CPS 234.

143. On 24 March 2023, BEN notified APRA of a material control weakness under paragraph 36 of CPS 234. In that notification, BEN stated that it would be undertaking a post-incident review in relation to the Cyber Attack which may identify other control weaknesses including compliance gaps in relation to CPS 234.

144. On 28 June 2023, BEN notified APRA of a CPS 234 breach in relation to the Cyber Attack (**Breach Report**) and attached a CPS 234 Breach Assessment (**Breach Assessment**). The Breach Assessment identified that the outcomes of the annual penetration testing performed since 2020 were not adequately escalated and reported to senior management to ensure the identified weaknesses were addressed in a timely manner.

L. POST INCIDENT REVIEWS FOLLOWING CYBER ATTACK

145. Following the Cyber Attack, BEN engaged CyberCX to conduct further penetration testing of the Ultracs system and to complete a Post Incident Review (**PIR**) of the Cyber Attack. The Board reviewed the CyberCX PIR and received briefings from management and CyberCX.

146. The penetration testing conducted following the Cyber Attack identified the same vulnerabilities that were identified in the Penetration Test Report.

147. Following the Cyber Attack, BEN prepared a response plan to address the recommendations made in the PIR (**Service One Incident Response Plan**).

(a) The Service One Incident Response Plan comprised 48 action items, each mapped to specific recommendations made by CyberCX.

(b) BEN implemented all 48 action items in the Service One Incident Response Plan by May 2024.

(c) On 4 July 2024, the Bank provided APRA with a summary on the actions taken pursuant to the Service One Incident Response Plan.

148. Between mid-2023 and October 2023, BEN conducted an internal review to assess the accountability of any of BEN's Accountable Persons for the Cyber Attack. The findings of the review included that:

(a) BEN's BMIT model was a key root cause for confusion with regards to responsibility for the management of IT security risk associated with the Alliance Bank internet banking platform;

(b) the Alliance Bank business unit was ultimately responsible for managing the risk associated with Ultracs, but did not have the requisite capability to properly understand and manage the IT risks, and relied on assistance from BEN's Technology & Transformation division where those capabilities resided at BEN;

(c) the findings from the Penetration Test Report should have been identified and reported as significant risks and escalated in accordance with the Operational Risk Framework, enabling those risks to be considered in an aggregated way; and

(d) it was possible that the Cyber Attack could have been avoided had the risks identified in the penetration test in 2020 been properly assessed, escalated and managed in line with BEN's

risk management frameworks and processes and had critical thinking been applied across all three lines of defence.

M. BEN ACCOUNTABLE PERSONS

M.1. BEN Accountable Persons – CTO

149. On and from 25 November 2019 to the end of the relevant period, BEN's CTO was an accountable person within the meaning of the BEAR.

150. From 5 November 2019 to 29 August 2022, the CTO's accountability statements included, under the heading "Information Technology frameworks and system management", responsibility for:

(a) management and delivery of BEN hosted IT operations, software, physical and cloud-based technology infrastructure; and

(b) direct business and function managed IT operations and systems so that these did not compromise the confidentiality, integrity or availability of the IT environment.

151. From 17 August 2020, the CTO's accountability statements added the qualification "excluding systems and software operated by specific business units" to the first of those responsibilities but did not identify the specific business units to which that exclusion referred.

152. In June 2022, BEN began a process of updating accountability statements of BEN's executives, including the CTO (**June 2022 Review**).

153. On 3 August 2022, an email was sent to BEN's executive team, including BEN's Chief Customer Officer, Consumer Banking and BEN's CTO. The email referred to an upcoming BEAR workshop to be held on 12 August 2022 with the executives and asked each executive to review the final drafts of their accountability statements, as well as "the exclusions to identify any gaps across the statements". The email attached a document titled "BEAR EoY Accountability Statement Review 02082022" (**2 August 2022 Slide Deck**).

154. The 2 August 2022 Slide Deck set out a series of limitations and exclusions for each accountable executive, along with the proposed executive who would inherit new accountabilities as a result of the exclusions. The entry for the CTO listed a series of explicit exclusions, including relevantly:

> "1. Support and maintenance of Business Managed IT for both known (refer list) and unknown applications including change management, access management, vulnerability

management, vendor management, backup and recovery, currency management, monitoring and incident management"

"6. IT Operations for Alliance Bank is excluded"

(the **Excluded Responsibilities**).

155. On 9 August 2022, BEN prepared an accountability map slide deck (**Accountability Map Slide Deck**). The Accountability Map Slide Deck identified the CTO as the senior executive responsible for information management, including information technology systems.

156. On 12 August 2022, BEN's executive team attended a BEAR accountability workshop as part of a meeting of the Executive Committee, at which the draft accountability statements were discussed.

157. On 19 August 2022, a further email was sent to BEN's executive team, attaching an updated version of the 2 August 2022 Slide Deck, titled "BEAR EoY AS Review120822_updated" (**19 August Slide Deck**). The email stated, in reference to the attachment, that "Slides 3-6 have been updated to reflect the discussion regarding Exceptions and Limitations, and decisions made post the session".

158. The 19 August Slide Deck page relating to the CTO's Excluded Responsibilities showed that the proposed accountable person for "6. IT Operations for Alliance Bank" as "Alliance Bank & CCO, Consumer (TBC)", with a comment added stating "12/08 - roles confirmed".

159. No further slide decks of the kind referred to in paragraphs 153 to 157 were prepared by BEN prior to the October 2022 Attacks and the Cyber Attack.

160. On or about 26 September 2022, the CTO signed an updated accountability statement, effective from 29 August 2022, which, for the first time, included a section titled "Limitations and Exclusions" which expressly excluded the Excluded Responsibilities.

161. The Excluded Responsibilities set out in the CTO's limitations and exclusions had not previously been used in BEN's accountability statements and were not directly included into the accountability statement of any other accountable person.

162. Following the Cyber Attack, the CTO's next signed accountability statement, dated 30 August 2023, no longer referenced the Excluded Responsibilities.

M.2. BEN Accountable Persons – Executive Rural Bank, Partnerships, Marketing & Corporate Affairs

163. From 1 July 2019 until about 1 February 2022, BEN's accountable persons within the meaning of the BEAR included an individual who, from 1 July 2019, was CEO Rural Bank, and then from 8 August 2019, was Executive Rural Bank, Partnerships, Marketing & Corporate Affairs (**Rural Bank Executive**).

164. The Rural Bank Executive's accountability statements included responsibility for aspects of the operations of Alliance Bank, being the management of models and arrangements for Alliance Bank and the execution of franchise models for Alliance Bank, but did not include any reference to responsibility for information technology operations, information security controls, or information technology systems used by or in connection with Alliance Bank.

165. The Rural Bank Executive's accountability statement dated 31 August 2020 did not include any reference to the "systems and software operated by specific business units" responsibility excluded from the CTO's statement on 17 August 2020 nor any reference to information technology, information security or IT systems.

M.3. BEN Accountable Persons – Chief Customer Officer

166. By February 2022, BEN's Chief Customer Officer (from 11 July 2022, its Chief Customer Officer, Consumer Banking) (**CCO**), was an accountable person within the meaning of the BEAR.

167. Following the departure of the Rural Bank Executive in February 2022, the CCO assumed responsibility for aspects of the operations of Alliance Bank.

168. The CCO's accountability statements referenced Alliance Bank in the scope of accountability in relation to:

(a) the distribution of products and services via Alliance Bank branches; and

(b) the management of distribution models, structures and arrangements for Alliance Bank,

but did not include any reference to responsibility for the IT operations of Alliance Bank.

169. As part of the June 2022 Review, BEN split accountabilities into core and role-based accountabilities, with core accountabilities introduced to all accountability statements. From

29 August 2022, the CCO's accountability statement contained the following relevant core accountabilities:

(a) Risk and compliance:

(i) Implementing, managing and monitoring compliance with BEN policies, legislation and regulatory requirements.

(b) Strategy, target and performance accountabilities:

(i) Identifying the need and approving the final solution for new systems and material changes to existing systems, for the Division and Business Unit's business processes and systems.

(ii) Service recovery and business continuity requirements, planning and testing for the division's business processes and systems in line with the Business Continuity Management Policy.

(iii) Ensuring the integrity of data collected, produced or processed by the division in accordance with the data governance framework.

170. From July 2022, the CCO's accountability statements also included a "Limitations and Exclusions" section, but at no time did any of the amended statements include any reference to responsibility for Alliance Bank IT operations or information security controls:

(a) the CCO's 11 July 2022 statement listed seven specific exclusions from the CCO's scope including Digital; and

(b) the CCO's 29 August 2022 statement did not include the Excluded Responsibilities, notwithstanding that the CTO's accountability statement of the same date expressly excluded these.

171. The Excluded Responsibilities referred to in the CTO's accountability statement dated 29 August 2022 were not directly allocated to the accountability statement of the CCO or to any other accountable person of BEN.

M.4. Accountability statement coverage from 29 August 2022 to 30 August 2023

172. The information technology operations for Alliance Bank constituted a part or aspect of the operations of BEN within the meaning of s 37D(1)(a)(i) of the Banking Act.

173. By at least August 2022, when the CTO's updated accountability statement excluded "Support and maintenance of Business Managed IT" and "IT Operations for Alliance Bank", it was unclear in the accountability statements which of BEN's accountable persons was responsible for information technology operations for Alliance Bank.

174. By reason of the matter set out at paragraph 154 above, from 29 August 2022, when the CTO signed an updated accountability statement with the Excluded Responsibilities, to 30 August 2023, no accountability statement of any of BEN's accountable persons covered responsibility for the information technology operations for Alliance Bank.

175. Notwithstanding the matter in paragraph 174 above, in practice the CTO and his direct report, the Chief Information Security Officer, took immediate responsibility for leading BEN's response to the Cyber Attack as described at paragraph 138 above.

N. BEN DID NOT ENSURE ACCOUNTABILITY COVERAGE

176. By reason of the matters set out at Section M above, from 29 August 2022 until the end of the relevant period, BEN did not ensure that the Excluded Responsibilities were covered by the accountability statement of an accountable person of BEN after they were excluded from the CTO's accountability statement, in that Alliance Bank information technology operations was not included in the accountability statements of any accountable person.

O. CONTRAVENTIONS ADMITTED BY BEN

177. In the circumstances referred to in Sections G-I above, between 2 June 2020 to June 2023, BEN failed to take reasonable steps to conduct the business of Alliance Bank with due skill, care and diligence in contravention of s 37C(a) of the Banking Act, by not having:

(a) adequate customer authentication controls for the prevention and detection of unauthorised access to, and unauthorised payments from, Alliance Bank customer accounts, as described in Section G.4 above;

(b) from 30 September 2020, when BEN had in force a CPS 234 Controls Testing Framework, a systematic testing program for the customer authentication controls applicable to Alliance Bank Digital Access, as described in Section H above; and

(c) appropriate governance and risk management for the information security of the Ultracs platform and TAS managed services that enabled Alliance Bank Digital Access, as described in Section I above.

178. By reason of the matters referred to in Sections M-N above, between 29 August 2022 to 30 August 2023, BEN failed to ensure that the responsibilities of the accountable persons of BEN and its subsidiaries covered all parts or aspects of the operations of BEN, and thereby contravened s 37D(1)(a)(i) of the Banking Act in that Alliance Bank information technology operations was not covered in the accountability statements of any accountable person, as described in paragraph 176 above.

P. OTHER MATTERS RELEVANT TO PENALTY

P.1. Prior conduct

179. BEN has not previously been found by the Court in proceedings under the Banking Act to have engaged in any similar conduct, or otherwise to have contravened a civil penalty provision.

P.2. Deliberateness

180. BEN did not deliberately engage in the conduct which resulted in the contraventions that are the subject of this Proceeding.

P.3. Contrition

181. BEN acknowledges and accepts responsibility for the conduct that gives rise to the contraventions the subject of the Proceeding.

182. On 14 March 2023, a statement was published on the Service One Website which included an unreserved apology to concerned members, and stated that Service One would be offering additional support to affected members, including free access to 'IDCARE'. Emails were also sent to Service One members on 11 March 2023, sincerely apologising for the inconvenience caused by the temporary disablement of internet banking services.

P.4. Cooperation

183. BEN has engaged constructively with APRA at all times since the Cyber Attack, including by:

(a) in addition to complying on 8 March 2023 with its obligation under paragraph 35 of CPS 234 to promptly notify APRA of the Cyber Attack:

(i) on 24 March 2023, notifying APRA of a material control weakness under paragraph 36 of CPS 234;

(ii) on 28 June 2023, submitting to APRA a breach assessment in respect of paragraphs 21 and 29 of CPS 234;

(iii) regularly and voluntarily updating APRA on its response to the Cyber Attack, its response on remediation and uplift to BEN's cyber risk management controls and capabilities to address the circumstances which contributed to the Cyber Attack and its broader uplift of BEN's IT risk and compliance, including in areas of cybersecurity and data governance; and

(b) in the course of APRA's investigation, and in addition to complying with its obligations to respond to the 12 statutory notices issued to it, voluntarily and proactively engaging with APRA, including by:

(i) disclosing to APRA the findings of its review to assess the accountability of any of BEN's Accountable Persons for the Cyber Attack, in November 2023;

(ii) providing to APRA a copy of an extended report prepared by CyberCX as part of the PIR referred to at paragraph 145 above on 19 June 2023; and

(iii) providing to APRA a copy of the Service One Incident Response Plan on 30 June 2023; and

(c) making admissions in relation to its conduct prior to filing the Originating Application and engaging with APRA on the preparation of this Statement of Agreed Facts and Admissions.

184. By its conduct, BEN has avoided the need for a contested proceeding on liability and penalty.

P.5. Size and resources of BEN

185. BEN is a medium sized ADI.

186. BEN is a regional bank that is significantly smaller than Australia's major banks (ANZ, NAB, Westpac and Commonwealth Bank) and Macquarie Bank, in terms of its revenue, net profit, total assets, and market capitalisation (as shown in the following table, which sets out the market capitalisation of each of the above-named banks as at close of market on 30 June 2026):

Bank	Market capitalisation ($B)
Commonwealth Bank of Australia (CBA)	275.3

Westpac Banking Corporation (WBC)	120.2
National Australia Bank Limited (NAB)	115.9
ANZ Group Holdings Limited (ANZ)	106.4
Macquarie Group Limited (MQG)	91.7
Bendigo and Adelaide Bank Limited	6.1

187. BEN's net profit (or loss) for each of the financial years ended 30 June 2020 to 30 June 2025 was as follows:

(a) $262.8 million during the financial year ending 30 June 2020;

(b) $524 million during the financial year ending 30 June 2021;

(c) $488.1 million during the financial year ending 30 June 2022;

(d) $497 million during the financial year ending 30 June 2023;

(e) $545 million during the financial year ending 30 June 2024; and

(f) ($97.1) million during the financial year ending 30 June 2025.

P.6. Loss and damage

188. No customer accounts were accessed in the October 2022 Attacks and there was no disruption to services. Accordingly, there was no loss or damage to Alliance Bank customers.

189. As referred to in paragraph 136(b) above, the Cyber Attack resulted in financial loss to a small number of Service One Alliance Bank customers by way of unauthorised transactions and withdrawals from their bank accounts. However, the financial loss was limited in time, given BEN fully refunded and remediated all impacted customers on or about 11 March 2023 (ie within four days) as set out in paragraph 136 above.

190. During and following the Cyber-Attack, BEN received approximately 218 complaints from Alliance Bank customers that its online banking and access had been restricted as a result of BEN's remediation attempts following the Cyber Attack. For a period of approximately seven days, Alliance Bank customers were limited to 'read only' access to online banking facilities, but

retained full access to banking via ATM, in-branch and telephone banking services and continued to be able to make payments via their credit and debit cards.

P.7. Benefit to BEN

191. BEN did not benefit, or stand to benefit, from the contravening conduct.

192. In responding to the Cyber Attack, BEN incurred costs of approximately $140,000 in remediating customer accounts and $610,000 engaging CyberCX, as described at paragraphs 136 and 145 above.

P.8. Remediation and uplift

193. By late 2021, the Bank had identified the operational risks inherent in the BMIT model and by June 2023, migrated all management responsibilities for BMIT assets to its Technology division. The migration of management responsibility of BMIT assets to the Technology division ensured that the lines of responsibility for those assets were unambiguous and that the assets were managed by personnel with appropriate expertise.

194. By June 2024, the Alliance Bank model had been discontinued, and all continuing Alliance Bank customers migrated to the Bank's core banking platform. The Bank has no ongoing relationship with Ultradata or TAS. The migration of Alliance Bank customers to the Bank's core banking platform had the effect that the risks posed by the deficiencies in the Alliance Bank customer authentication controls (and the testing and governance of those controls) for online banking at Alliance Bank were no longer present.

195. In addition to the remedial actions implemented immediately following the Cyber Attack and in accordance with the Service One Incident Response Plan described at paragraph 147 above, the Bank has implemented a group-wide uplift program to its cyber risk management controls and capabilities, including:

(a) decommissioning the BMIT model, consolidating core banking platforms to a single platform;

(b) moving to a ‘Zero Trust’ information security architecture involving continuous verification, least privilege access, and segmentation of critical assets;

(c) identifying and understanding the evolving cybersecurity threat landscape in order to protect the Bank, its customers and the community, including by engaging CyberCX to conduct a

review of emerging threats and major threat actors to allow the Bank to identify any immediate weaknesses and security risks;

(d) appointing a new Chief Information Security Officer responsible for preparing a new Enterprise Security Strategy for the Bank;

(e) designing and implementing a Data Management Framework and Data Custodian Program, which includes a data governance tool with a central register, an enterprise-wide data literacy program, identification and management of critical data elements and data architecture; and

(f) expanding its partnership with Google Cloud in a multi-year agreement that will migrate operations to Google Security Operations and Google Security Command Centre, further improving BEN's information security measures including the ability to detect, investigate and respond to threats.

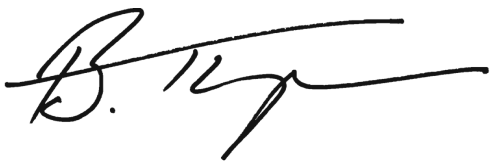
Date: 10 August 2026

……..

Signed by Alana Giles

Holding Redlich

Solicitor for the Applicant



……..

Signed by Belinda Thompson

Allens

Solicitor for the Respondent