PRIVACY ACT 1988 (CTH) Undertaking to

the Australian Information Commissioner

under

section 114 of the *Regulatory Powers (Standard Provisions) Act 2014* (Cth)

This Undertaking is given to the Australian Information Commissioner (**Commissioner**) by Commonwealth Bank of Australia ACN 123 123 124 (**CBA**).

1 Definitions and Interpretation

1.1 Definitions

In addition to terms defined elsewhere in this Undertaking, the following definitions apply:

Activities means each of the obligations imposed on CBA under paragraph 8 of this Undertaking.

Activity Completion Report has the meaning set out in paragraph 16(a)(ii)(A) of this Undertaking.

Agreed Work Plan has the meaning set out in paragraph 12(b)(iii)(A) of this Undertaking.

APPs means the Australian Privacy Principles set out in Schedule 1 to the Privacy Act.

Assurance Plan means, in respect of any financial year, a plan setting out CBA's scheduled assurance activities for that financial year.

CBA Banking Services means any business conducted by CBA, or by a subsidiary of CBA, that provides banking or financial products and services to consumers in Australia, but excluding:

(a) any financial planning services that are not provided under the 'Commonwealth Financial Planning' brand;

(b) any products or services provided by, or operations conducted under, the 'Bankwest' brand; and

(c) any products or services provided, or operations conducted, by a CBA Excluded Subsidiary

CBA customer means any customer of CBA Banking Services, or any person who has at any time been a customer of CBA Banking Services or any person who has provided any personal information to CBA or any Related Body Corporate of CBA in connection with a proposal to become a customer of CBA Banking Services, whether or not that person becomes a customer of CBA Banking Services.

CBA Excluded Subsidiary means:

(a) any subsidiary of CBA incorporated in a jurisdiction other than Australia;

(b) any subsidiary of CBA in respect of which CBA does not (directly or indirectly) hold a 100% ownership interest;

(c) Residential Mortgage Group Limited and its subsidiaries;

(d) Australian Investment Exchange Limited; and

(e) AHL Holdings Pty Limited and its subsidiaries.

CBA IT Service means an information technology service, comprising systems, applications and hardware (or any one or more of them), which is used by CBA to support a business process for, or related to, CBA Banking Services (whether or not used by CBA for any other purpose).

CBA Key Applications has the meaning set out in paragraph 8.3 of this Undertaking.

CMLA means The Colonial Mutual Life Assurance Society Ltd, ABN 12 004 021 809.

CMLA Related Remedial Work means each of the obligations imposed on CBA under paragraph 9 of this Undertaking.

Commencement Date means the date on which this Undertaking, executed by CBA, is accepted by the Commissioner.

Contractor means a third party that:

(a) is a party to a contract with CBA for the supply of products or services to CBA Banking Services (**CBA Contract**); and

(b) accesses or holds personal information of CBA customers, or any sensitive information, for the purpose of performing its obligations under the CBA Contract.

Data Access Logging Mechanisms means the mechanisms implemented by CBA to record access by CBA employees to the CBA Key Applications, the CBA IT Services and any other systems, applications and customer records (or any one or more of them).

Data Incidents means the 2016 Data Incident and the 2018 Data Access Issue.

Enforceable Undertaking or **Undertaking** means this written undertaking given to the Commissioner by CBA under section 114 of the Regulatory Powers Act and for the avoidance of doubt includes all schedules.

GDW has the meaning set out in Confidential Schedule 1 to this Undertaking.

Independent Expert has the meaning set out in paragraph 10(a) of this Undertaking.

Material Change means any change to the Agreed Work Plan that:

(a) is, or (in CBA's opinion) is likely to result in, an extension to a timeframe within which an Activity is to be completed;

(b) would result in any material change to the actions that would be taken by CBA to complete an Activity; or

(c) would result in any Activity being excluded from the Agreed Work Plan, or any modification to the scope or nature of an Activity for the purposes of the Agreed Work Plan.

OAIC means the Office of the Australian Information Commissioner.

Policy means CBA's internal privacy policy, which sets out high-level principles that govern the decision-making and conduct of CBA and its employees in relation to CBA's obligations under the Privacy Act.

Privacy Act means the *Privacy Act 1988* (Cth).

Privacy Procedures means CBA's business and support unit privacy procedures, which outline operational steps or processes for complying with the Policy.

Progress Report has the meaning set out in paragraph 14 of this Undertaking.

Proposed Activity Completion Date means:

(a) in respect of the Activities set out at paragraph 8.1 to paragraph 8.5 (inclusive), the date which is 36 months after the Commencement Date; or

(b) in respect of the Activities set out at paragraph 8.6, the date which is 48 months after the Commencement Date.

Regulatory Powers Act means the *Regulatory Powers (Standard Provisions) Act 2014* (Cth).

Related Body Corporate has the meaning given to that term in the *Corporations Act 2001* (Cth).

Retention Standard means CBA's record retention standards, which set the standards for the retention and disposal of records (including records, in any format, containing personal information) by CBA.

Revised Work Plan has the meaning set out in paragraph 12(c) of this Undertaking.

Sensitivity and Security Classification Controls means CBA's controls (both technical and procedural) to assign and record the classification of CBA's information assets (including personal information).

Term means the period from, and including, the Commencement Date to, and including, the date on which CBA provides the report of the audit under paragraph 17 to the Commissioner.

User Access Controls means the controls (both technical and procedural), by which CBA grants, monitors and restricts access by CBA employees to the CBA Key Applications, the CBA IT Services and any other systems, applications and customer records of CBA (or any one or more of them).

User Access Profiles means the access rights and privileges associated with a particular role of a CBA employee.

Work Plan has the meaning set out in paragraph 11(a) of this Undertaking.

2016 Data Incident means the data incident described in paragraph 3.1 of this Undertaking.

2018 Data Access Issue means the data access issue described in paragraph 3.2 of this Undertaking.

1.2 Interpretation

Unless the contrary intention appears:

(a) terms defined in the Privacy Act have the same meaning in this Enforceable Undertaking as they have in the Privacy Act;

(b) the words **includes**, **including**, and similar expressions are not used as, nor intended to be interpreted as, words of limitation;

(c) a reference to time is a reference to Sydney, Australia time;

(d) a reference to a day is a calendar day, and to be interpreted as the period of time commencing at midnight and ending 24 hours later; and

(e) a reference to a month is a calendar month.

2 Background

(a) CBA is a body corporate incorporated in Australia, and an organisation within the meaning of section 6C of the Privacy Act.

(b) CBA engages in the business of providing banking services to customers, including to individuals, in Australia and elsewhere. CBA holds personal information and is required by the Privacy Act to, among other things, take reasonable steps to:

(i) implement practices, procedures and systems relating to CBA's functions or activities that will ensure CBA complies with the APPs in respect of that information, as required by APP 1.2;

(ii) protect personal information CBA holds from misuse, interference and loss, and from unauthorised access, modification or disclosure, as required by APP 11.1; and

(iii) destroy or de-identify personal information that CBA no longer needs for any purpose, nor is required to retain under an Australian law, or a court/tribunal order, as required by APP 11.2.

3 Data Incidents Background

3.1 2016 Data Incident

(a) On 21 April 2016, a vendor of CBA dispatched two magnetic data tapes containing historical CBA customer statements to its supplier for secure destruction.

(b) Following CBA's request for destruction certificates, on 9 May 2016, the vendor advised CBA that the data tapes were missing, prompting CBA to mobilise its incident response team and to commence an independent forensic investigation into the loss.

(c) CBA also implemented heightened security monitoring of customer accounts as a precaution against suspicious account activity.

(d) Despite comprehensive enquiries, CBA was unable to confirm the secure destruction of the data tapes. The independent forensic investigation concluded that the most likely scenario was that the package containing the data tapes had been disposed of.

(e) The OAIC considered the information provided by CBA to the OAIC in relation to the 2016 Data Incident in June and October 2016 and determined in October 2016 that it would not take further regulatory action at that time.

3.2 2018 Data Access Issue

(a) In August 2018, CMLA (the life insurance subsidiary of CBA) informed the OAIC that, during the course of the data segregation activities for its sale, it had identified that certain shared applications within the CBA group contained information of a sensitive nature relating to CMLA customers, including sensitive information and government related identifiers. This information was accessible in some form to some CBA group employees who were not employees working within CMLA. CMLA identified 16 shared applications which contained the CMLA customer information described above.

(b) On discovering this issue, CBA and CMLA commenced remedial action in respect of the 16 applications to segregate the information described in subparagraph (a) above and implement appropriate access controls to restrict access to that information by any CBA group employees who were not employees working within CMLA.

(c) CBA is undertaking an investigation, with the assistance of an independent expert, McGrathNicol Advisory, to determine whether the CMLA customer information contained in the 16 applications (and described in subparagraph (a) above) had been subject to unauthorised access by non-CMLA employees. As at the date of this Undertaking, that investigation is ongoing and CBA has not identified any instances of unauthorised access by CBA group employees to this information.

4 The OAIC's Response to the Data Incidents

(a) The OAIC has undertaken preliminary inquiries under s 42(2) of the Privacy Act in relation to the Data Incidents over the period since May 2018.

(b) The OAIC has notified CBA that, as a result of its preliminary inquiries, it has concerns arising from the Data Incidents, which indicate deficiencies in CBA's management of personal information, namely:

(i) the 2016 Data Incident raises issues with CBA's compliance with APP 1.2 and APP 11.2; and

(ii) the 2018 Data Access Issue raises issues with CBA's compliance with APP 1.2 and APP 11.1.

5 Acknowledgment

(a) CBA has cooperated with the OAIC and responded to the OAIC's preliminary inquiries in relation to the Data Incidents.

(b) CBA has also undertaken, and is undertaking, certain remedial action with the aim of ensuring that incidents similar to the Data Incidents do not recur.

(c) CBA, however, acknowledges the Commissioner's concerns regarding the Data Incidents. Accordingly, CBA offers this Enforceable Undertaking to the Commissioner under section 114 of the Regulatory Powers Act to address those concerns.

6 Undertaking limited to matters expressly dealt with

The only obligations CBA is required to perform pursuant to this Undertaking are those expressly set out in this Undertaking.

7 Term of Undertaking

(a) This Undertaking continues for the Term.

(b) If at any time CBA, acting reasonably, determines that it is unlikely to complete the:

(i) Activities by the applicable Proposed Activity Completion Date; or

(ii) CMLA Related Remedial Work by the date specified in paragraph 9,

CBA will notify the Commissioner within 14 days of such determination.

(c) If CBA notifies the Commissioner under paragraph 7(b), the parties will negotiate in good faith to agree any amendments to this Undertaking that are reasonably necessary to ensure that CBA completes the relevant Activities, or the CMLA Related Remedial Work (as applicable), as soon as practicable and, if practicable, prior to the applicable timeframe referred to in subparagraph (b) above. The Commissioner retains full discretion to determine whether or not to agree to any such amendments and may take any action she determines is necessary following a notification to the Commissioner under paragraph 7(b), including applying to the Federal Court of Australia for an order under section 115 of the Regulatory Powers Act.

8 Activities

This Undertaking requires CBA to complete each of the Activities set out in this paragraph 8 by the applicable Proposed Activity Completion Date.

8.1 Policy, Privacy Procedures and Retention Standard

(a) CBA will:

(i) undertake a review of the Policy, and implement any changes to the Policy that are necessary to ensure it sets out the:

(A) requirements under the Privacy Act, as they apply to CBA Banking Services, that must be met by CBA and its employees; and

(B) accountabilities of CBA employees to ensure such compliance; and

(ii) prepare a written version of the Privacy Procedures for CBA Banking Services, which specify the operational steps and processes to be implemented by CBA Banking Services and its employees to ensure compliance with the Policy (as amended in accordance with paragraph 8.1(a)(i)).

(b) CBA undertakes to:

(i) engage an appropriately qualified external expert to provide advice on CBA's obligations to retain personal information that is collected or held for the purposes of CBA Banking Services; and

(ii) having regard to the external expert's advice under paragraph 8.1(b)(i), review the Retention Standard as it applies to CBA Banking Services, and implement any changes to the Retention Standard that are necessary to ensure CBA Banking Services' practices relating to the retention or disposal of records containing CBA customer personal information comply with the Privacy Act.

(c) CBA will operationalise the Policy, Privacy Procedures and Retention Standard (in each case as amended in accordance with this paragraph 8.1) in CBA Banking Services by:

(i) updating and documenting CBA Banking Services' controls to meet the control objectives set out in the Privacy Procedures and Retention Standard (which may include manual or automated environments). Where no controls exist as part of CBA Banking Services' existing controls, CBA Banking Services will follow its existing operational and compliance risk management frameworks to record and remediate any controls gaps to meet the control objectives set out in the Privacy Procedures and Retention Standard taking into account that the level of automated controls will be dependent on (among other things) business processes in CBA Banking Services;

(ii) using its best endeavours to increase awareness of, and providing training on, the Policy, Privacy Procedures and Retention Standard to directors of CBA and to all CBA employees working within CBA Banking Services who may have access to CBA customer personal information in the course of performing their duties; and

(iii) making the Policy, Privacy Procedures and Retention Standard accessible to all CBA employees working within CBA Banking Services, including on CBA's internal website and by providing copies of the Policy, Privacy Procedures and Retention Standard, and any amendments to those documents, to its directors.

(d) commencing on and from 1 July 2020, and for the remaining Term of this Undertaking, CBA will include in each of its CBA Banking Services' Assurance Plans, and implement, an annual review of compliance by CBA Banking Services with the Policy, Privacy Procedures and Retention Standard. CBA will, as soon as is practicable, take action to remedy any non-compliance that is identified as a result of any such annual review.

8.2 Privacy Impact Assessments

CBA will:

(a) undertake a review of its existing privacy impact assessment process having regard to the Privacy Act and the OAIC's *Guide on undertaking privacy impact assessments* (dated May 2014), implement any changes to that privacy impact assessment process that will assist CBA's compliance with the Privacy Act and will specify when a privacy impact assessment is required in the Privacy Procedures;

(b) incorporate the privacy impact assessment process (including any amendments to that process as a result of the review under subparagraph (a) above) into CBA Banking Services' existing risk and controls management processes; and

(c) use its best endeavours to ensure that CBA employees working within CBA Banking Services undertake privacy impact assessments as required by the Privacy Procedures (as updated in accordance with paragraph 8.1).

8.3 CBA Key Applications

For the applications listed in Confidential Schedule 1 (**CBA Key Applications**), CBA undertakes to:

(a) review the existing User Access Controls that protect personal information held in CBA Key Applications and implement any changes to those User Access Controls that are necessary to ensure access to such information is limited to those User Access Profiles that are permitted to have such access, having regard to the Privacy Act, including in particular APP 11.1;

(b) implement an annual review of User Access Profiles that apply to each CBA Key Application, including the personal information access privileges assigned to those User Access Profiles;

(c) design and implement a review process to assess each CBA employee's continued eligibility in respect of User Access Profiles (which authorise access to applications and personal information held in CBA Key Applications). CBA will ensure that this review process will be undertaken each time a change in the position of any CBA employee occurs (at or before the time that change occurs);

(d) based on the findings of each of the reviews under subparagraphs (b) and (c) above, remove any users identified, as at the date the relevant review is completed, as not requiring access to the relevant CBA Key Applications;

(e) review the Sensitivity and Security Classification Controls that apply to the classification of personal information held in CBA Key Applications at the date of review (such controls to be further defined in the Agreed Work Plan) and implement all necessary changes to those Sensitivity and Security Classification Controls which are required to ensure compliance by CBA with APP 11.1;

(f) review CBA's existing Data Access Logging Mechanisms that log access to CBA customer personal information held in CBA Key Applications (such mechanisms to be further defined in the Agreed Work Plan) (the **Access Logs**), and implement all necessary changes to:

  (i) ensure the Access Logs are subject to specific retention periods;

  (ii) identify the User Access Profiles that are permitted to access the Access Logs; and

  (iii) ensure that Access Logs are available to those User Access Profiles identified under subparagraph (f)(ii) above for the purpose of undertaking investigations into suspected incidents of unauthorised access to personal information held in CBA

Key Applications and for use in connection with CBA's internal user behaviour analytics technology; and

(g) apply CBA's internal user behaviour analytics technology to CBA Key Applications to assist CBA in identifying potentially suspicious application-user behaviour, which may be indicative of inappropriate access to information held in a CBA Key Application.

8.4 Contractors

CBA undertakes to:

(a) review the privacy risk management and monitoring processes that apply to Contractors and implement changes to those processes to ensure that CBA complies with its obligations under the APPs;

(b) implement reasonable monitoring of each Contractor's compliance with its contractual obligations to CBA governing the handling of personal information (including reasonable monitoring of compliance with any contractual obligation to destroy or de- identify personal information) having regard to the rights of CBA under the relevant contract as to the manner in which it may monitor the Contractor's compliance with such obligations; and

(c) ensure that each Contractor undertakes to provide, or procure the provision of, privacy training to its employees who may have access to personal information of CBA customers in the course of performing any contract with CBA for the supply of products or services to CBA Banking Services.

8.5 Data Tapes

To address its compliance with APP 11.2, CBA will:

(a) use best endeavours to identify magnetic data tapes within the control or possession of CBA Banking Services which CBA reasonably believes contain unknown or unreadable content, or CBA customer personal information;

(b) if CBA identifies any data tapes under subparagraph (a) above, determine (if appropriate, after obtaining external expert advice) whether any of the identified data tapes must be destroyed, or any customer personal information thereon de-identified or destroyed, having regard to the content of those tapes and APP 11.2 as it applies to CBA Banking Services; and

(c) where an identified data tape should be destroyed, or customer personal information thereon de-identified or destroyed, use its best endeavours to procure the secure destruction of the relevant data tape, or the de-identification or destruction of the customer personal information contained on the relevant data tape.

8.6 CBA Customer Systems and Applications

CBA undertakes to:

(a) identify all CBA IT Services that collect or hold any personal information of CBA customers (**CBA Customer Systems and Applications**);

(b) appoint the Independent Expert to rank each CBA Customer System and Application in order of risk, having regard to:

(i) the risk of access to the relevant CBA Customer System and Application by CBA employees, for whom access to the CBA Customer System and Application is not reasonably necessary for the performance of their duties; and

(ii) the sensitivity and volume of CBA customer personal information collected or held by the relevant CBA Customer System and Application; and

(c) appoint the Independent Expert to prepare a plan that, having regard to the ranking of each CBA Customer System and Application completed by the Independent Expert in accordance with subparagraph (b):

(i) specifies, in respect of each CBA Customer System and Application, any action that CBA should take to ensure compliance by it with APP 11.1 in relation to the personal information that is collected or held in that CBA Customer System and Application (**Systems and Applications Process**); and

(ii) specifies the timeframes for the performance of the Systems and Applications Process; and

(d) complete the Systems and Applications Process, in a staged manner, and in accordance with the plan prepared under subparagraph 8.6(c) above.

9 CMLA Related Remedial Work

CBA undertakes to procure the performance of the user access review set out in Item 1 of Confidential Schedule 2 in respect of the applications set out in Item 2 of Confidential Schedule 2 within 30 days of the completion of the sale of CMLA and provide the findings of the review to the Commissioner within 30 days of the review's completion.

10 Engagement of Independent Expert

(a) Within 14 days of the Commencement Date, CBA will engage a suitably experienced and qualified independent external person, approved by the Commissioner (the **Independent Expert**), to undertake the tasks set out in paragraph 10(c) of this Undertaking.

(b) CBA will ensure that the person engaged to be the Independent Expert under paragraph 10(a) is a reputable forensic practice operating in Australia with specialists in audit, information technology, data storage and cyber security, and with sufficient available resources to complete the tasks referred to in paragraph 10(c).

(c) The Independent Expert will be responsible for:

(i) undertaking the tasks allocated to it under paragraph 8.6;

(ii) reviewing the Work Plan, and any Revised Work Plan, and confirming the Agreed Work Plan subject to the process set out in paragraph 12;

(iii) providing CBA and the Commissioner with six monthly Progress Reports on CBA's progress against the Agreed Work Plan in accordance with paragraph 14;

(iv) providing CBA with Activity Completion Reports, and other reports, in accordance with paragraph 16;

(v) completing the audit described in paragraph 17; and

(vi) carrying out any other tasks allocated to it under this Undertaking, or by CBA, for the purposes of this Undertaking.

(d) CBA undertakes to provide to the OAIC, within 21 days of the Commencement Date, a copy of the terms of engagement pursuant to which the Independent Expert is engaged to undertake the tasks set out in this Undertaking.

11 Agreed Work Plan

Within 90 days of the Commencement Date, CBA will:

(a) prepare a work plan, the objective of which must be the completion of all of the Activities, in an appropriately staged manner, by the applicable Proposed Activity Completion Date and, where relevant, within the timeframes set out in paragraph 8 (**Work Plan**); and

(b) confirm the Work Plan with the Independent Expert in accordance with the process set out in paragraph 12 of this Undertaking.

12 Agreed Work Plan Confirmation Process

(a) CBA will provide the Work Plan to the Independent Expert setting out:

(i) the action CBA will take to ensure completion of the Activities;

(ii) timeframes within which each of the Activities will be completed in order to ensure that CBA is able to complete the Activities by the applicable Proposed Activity Completion Date and, where relevant, within the timeframes set out in paragraph 8; and

(iii) who will be accountable within CBA for delivering on each action in subparagraph (i) above within the timeframes specified in subparagraph 12(a)(ii).

(b) CBA will require the Independent Expert to, not later than 14 days after receipt of the Work Plan under paragraph 12(a):

(i) consult with the Commissioner regarding the Work Plan;

(ii) complete its review of the Work Plan, taking into consideration its consultation with the Commissioner, to assess whether completion of the actions in the Work Plan will result in completion of the Activities by the applicable Proposed Activity Completion Date and, where relevant, within the timeframes set out in paragraph 8; and

(iii) either:

(A) provide CBA with written confirmation that completion of the actions in the Work Plan will result in completion of all of the Activities by the applicable Proposed Activity Completion Date and, where relevant, within the timeframes set out in paragraph 8, in which case the Work Plan will become the Agreed Work Plan; or

(B) provide a written report to CBA that identifies any deficiencies in the Work Plan, and provide recommendations to address those deficiencies (**Work Plan Report**).

(c) Where the Independent Expert has provided a Work Plan Report, CBA undertakes to provide the Independent Expert with a revised Work Plan (**Revised Work Plan**) within 7 days after the date on which it receives the Work Plan Report, which:

(i) incorporates (in addition to the content set out under paragraph 12(a)) the actions CBA proposes to take to address the deficiencies identified in the Work Plan Report; and

(ii) in respect of any recommendations identified in the Work Plan Report which CBA will not implement, provide reasons and, where appropriate, reasonable alternative action that CBA proposes to take to address the relevant deficiencies identified in the Work Plan Report.

(d) Within 5 days of the Independent Expert's receipt of a Revised Work Plan under paragraph 12(c), the process in paragraphs 12(b), and 12(c) will be repeated in respect of the Revised Work Plan as if it were the Work Plan.

(e) CBA will provide a copy of the Agreed Work Plan to the Commissioner within 7 days of the date it is confirmed by the Independent Expert in accordance with this Undertaking.

(f) CBA will prepare a summary of the Agreed Work Plan (excluding any content that is confidential information), setting out at a high-level the proposed steps CBA will take to complete the Activities and the timetable for completion of the Activities (**Summary**). CBA will make the Summary publicly available on its website.

13 Material Changes to Agreed Work Plan

(a) If CBA wishes to make a Material Change to the Agreed Work Plan, CBA must submit the proposed Material Change to the Independent Expert and the Commissioner in writing, including reasons for the Material Change and any other information that CBA wishes to include.

(b) The Independent Expert must, within 7 days of receipt of a proposed Material Change under paragraph 13(a), consult with the Commissioner regarding the proposed Material Change, assess the proposed Material Change (taking into consideration its consultation with the Commissioner) and advise CBA (copied to the Commissioner) whether the proposed Material Change is, in the Independent Expert's view, reasonably necessary for CBA to comply with its obligations under this Undertaking.

(c) Where the Independent Expert provides a written confirmation in respect of a proposed Material Change under paragraph 13(b) confirming that it has determined that the proposed Material Change is reasonably necessary for CBA to comply with its obligations under this Undertaking, the Agreed Work Plan is varied accordingly.

(d) Following a variation to the Agreed Work Plan in accordance with subparagraph (c) above, CBA will promptly update the Summary to the extent necessary to ensure it is accurate, and will make the updated Summary publicly available on its website.

(e) For the avoidance of doubt, nothing in this paragraph 13 limits the operation of paragraph 7 of this Undertaking.

14 Progress Reports

The Independent Expert will provide CBA and the Commissioner with a report on a 6 monthly basis setting out for the preceding 6 month period:

(a) CBA's progress against the actions in the Agreed Work Plan; and

(b) all changes made by CBA to the Agreed Work Plan (**Progress Reports**),

with the first Progress Report to be provided on the date which is 6 months after the Commencement Date.

15 Activity Completion Statement

CBA undertakes to provide written confirmation to the Independent Expert and the Commissioner within 14 days of completion of an Activity or, if CBA has grouped two or more Activities into an Activity group (**Activity Group**), within 14 days of completion of an Activity Group. CBA undertakes to provide written confirmation to the Independent Expert and the Commissioner that CBA has completed the relevant Activity or Activities (**Activity Completion Statement**).

16 Activity Completion Report

(a) The Independent Expert will, within 14 days after receipt of an Activity Completion Statement under paragraph 15 (or such later date as agreed between the OAIC and CBA and notified to the Independent Expert):

(i) assess whether CBA has completed the relevant Activity or Activities; and

(ii) either:

(A) provide CBA and the Commissioner with a written report confirming that CBA has completed the relevant Activity or Activities (**Activity Completion Report**); or

(B) provide CBA and the Commissioner with a written report if it identifies that the relevant Activity or Activities have not been completed in accordance with the Undertaking and recommend reasonable timeframes for the completion of the Activity or Activities.

(b) Where the Independent Expert has provided a report under paragraph 16(a)(ii)(B), CBA undertakes to complete the relevant Activity or Activities within the timeframes specified in that report, and provide a revised Activity Completion Statement to the Independent Expert and the Commissioner within 7 days of completion of the relevant Activity.

(c) Following receipt of the revised Activity Completion Statement, the Independent Expert will, within 7 days of receipt, repeat the process set out in paragraph 16(a) in respect of the revised Activity Completion Statement as if it were the relevant Activity Completion Statement.

17 Audit of Compliance

(a) Not later than 6 months after the final Activity Completion Report is provided by the Independent Expert to CBA, CBA will procure the Independent Expert to undertake and complete an audit of CBA Banking Services to determine whether the actions taken by CBA in respect of the Activities have been operationalised, which will include an audit of compliance by CBA Banking Services with the Policy, Privacy Procedures and Retention Standard.

(b) Within 14 days of receipt of the report of the audit, CBA will provide the report of the audit to the Commissioner.

18 Provision of Information

(a) CBA will provide relevant documents and information requested by the Commissioner from time to time within 14 days of written request (or such later date as agreed between the OAIC and CBA) by the Commissioner for the purpose of assessing CBA's progress in complying with this Undertaking.

(b) The Commissioner and OAIC acknowledge that the Independent Expert's reports or audit findings, information and reports relating to the CMLA Related Remedial Work and the CBA Customer Systems and Applications, the Work Plan, the Agreed Work Plan, Progress Reports, Activity Completion Statements, Activity Completion Reports, Confidential Schedule 1, Confidential Schedule 2, and any other information that is provided by CBA, or the Independent Expert, in accordance with this Undertaking, are likely to contain CBA's sensitive commercial information and security protocols and which is not publicly available information (such information and protocols being commercial-in-confidence information) which, if publicly disclosed, has the potential to undermine the security of CBA's information technology systems and of the personal information it holds.

(c) The Commissioner and the OAIC will only:

(i) disclose the commercial-in-confidence information with CBA's written agreement, unless required in response to a request from a House or Committee of the Commonwealth Parliament or otherwise required by law; and

(ii) use the commercial-in-confidence information for the Commissioner's privacy regulatory activities.

19 Further Acknowledgments

(a) CBA agrees that the Commissioner:

(i) will publish this Undertaking on the Commissioner's website;

(ii) may publicly refer to this Undertaking, including any breach of this Undertaking by CBA;

(iii) may issue media releases or social media posts and undertake media interviews (or authorise any other OAIC officer to undertake media interviews) on acceptance of this Undertaking, referring to its terms and the circumstances of its acceptance by the Commissioner; and

(iv) may, if she considers that CBA has breached this Undertaking, apply to the Federal Court of Australia for an order under section 115 of the Regulatory Powers Act.

(b) CBA recognises that this Undertaking does not derogate from the rights and remedies available to any individual arising from either of the Data Incidents.

Executed by:

……
Signature of Authorised Signatory

……
Name of Authorised Signatory

……....
Title of Authorised Signatory

Witnessed by:

……..
Signature of Witness

……..
Name of Witness

Commonwealth Bank of Australia ACN 123 123 124

Dated:

Accepted by:

Australian Information Commissioner pursuant

to section 114 of the Regulatory Powers Act

Dated: