Form 59
Rule 29.02(1)

Affidavit

No. NSD719 of 2020

Federal Court of Australia

District Registry: NSW

Division: General

Etienne Alexiou

Applicant

Australia and New Zealand Banking Group Limited (ACN 005 357 522)

Respondent

Affidavit of: **David Joseph Mulligan**

Address: 833 Collins Street, Docklands, Victoria 3008

Occupation: Engineer

Date: 17 November 2023

Contents

Filed on behalf of (name & role of party) Australia and New Zealand Banking Group Limited, the Respondent
Prepared by (name of person/lawyer) Michael Tamvakologos
Law firm (if applicable) Seyfarth Shaw Australia
Tel 03 9613 0712 Fax 03 9631 0790
Email mtamvakologos@seyfarth.com
Address for service (include state and postcode) Seyfarth Shaw Australia
Level 27, 55 Collins Street, Melbourne VIC 3000

[Version 3 form approved 02/05/2019]

Document number	Details	Paragraph	Page
6	Annexure '**DJM-5**', being a copy of the email from the Quarantined Emails Enquiries team to Etienne dated 9 February 2012	36	27

I, David Joseph Mulligan, of business address 833 Collins Street, Docklands, Victoria 3008, Engineer, say on oath:

1. I am employed by the Respondent, Australia and New Zealand Banking Group Limited (**ANZ**), in the position of Engineer, Threat Intelligence & Offensive Security.

2. I make this affidavit from my own knowledge, save where otherwise indicated. Where I depose to matters on the basis of information provided to me by other persons, I believe that information to be true.

3. References in this affidavit to the **Relevant Period** are references to the period from 1 July 2011 to 30 September 2015.

Employment history with ANZ

4. In January 2012, I commenced employment with ANZ in the role of Senior Technical Consultant in the Windows System Management – Messaging team. In this role, I was responsible for managing and supporting ANZ's email, fax and mobility infrastructure.

5. I have held the following roles since the start of my employment with ANZ:

   (a) From January 2016 to October 2018 – Senior Security Consultant;

   (b) From October 2018 to April 2020 – Analyst;

   (c) From April 2020 to March 2021 – Cloud Security Analyst; and

   (d) From March 2021 to July 2021 – Red Team Analyst.

6. I have held my current role of Engineer, Threat Intelligence & Offensive Security, since July 2021. My main responsibility in this role is the performance of offensive security and red teaming, the purpose of which is to test ANZ's information technology (**IT**) security systems for vulnerabilities. "Red teaming" is the process of simulating a cyberattack on an organisation's security systems to identify potential vulnerabilities.

Monitoring of inbound and outbound emails during the Relevant Period

7. At all times during the Relevant Period, ANZ had email security systems in place to monitor both emails sent from external parties to the ANZ corporate email accounts of ANZ employees (i.e. inbound emails), and emails sent by ANZ employees from their ANZ corporate email accounts to external parties (i.e. outbound emails), for inappropriate and malicious content.

8. When I commenced employment with ANZ in January 2012, ANZ used an email security system called Symantec MessageLabs (**MessageLabs**) to monitor inbound emails for inappropriate and malicious content.

9. Before MessageLabs was introduced in December 2011, ANZ used an email security system called M86 MailMarshal (**MailMarshal**) to monitor inbound emails. I am aware that ANZ used MailMarshal because, in my role as Senior Technical Consultant in the Windows System Management – Messaging team, I supported the inbound email infrastructure and the transition the MessageLabs system and processes.

10. Although MailMarshal was replaced by MessageLabs with respect to the monitoring of inbound emails, ANZ continued to use MailMarshal to monitor outbound emails for inappropriate and malicious content up until about 2013. After that time, ANZ started using MessageLabs to monitor outbound emails. ANZ moved to MessageLabs because MailMarshal was becoming inadequate for the increasing volume of emails that passed through it.

11. Email monitoring by both MailMarshal and MessageLabs was an automated process during the Relevant Period. Inbound and outbound emails passed through either MailMarshal or MessageLabs for filtering before being delivered into a recipient's mailbox. Emails were filtered to identify any keywords that were on a list of identified keyword terms. The keyword terms were routinely reviewed by the Quarantined Email Enquiries team, which was part of ANZ's security team. The purpose of the identified keyword terms was to capture swear words and other inappropriate language and variations of them, such as a word where a number, symbol or shorthand was used to replace a letter. I cannot locate copies of the lists of identified keyword terms that were used during the Relevant Period. However, I recall that examples of keywords included "shit" and "fuck" and variations of those words such as "$hit" and "fuk".

12. During the Relevant Period, MailMarshal and MessageLabs used different approaches to identify and quarantine emails. However, the end result of both email security systems was the same in that, if any part of the subject line or body of an email was identified as containing a keyword or keywords on the list of identified keyword terms that met specified criteria, the email was quarantined and as a result not delivered to the recipient's mailbox.

13. During the Relevant Period, if an inbound or outbound email was quarantined, the ANZ employee (as either the recipient or the sender of the email) received an automated email saying that the email had been quarantined. The employee could then raise a request to have the email released from quarantine by emailing the Quarantined Emails Enquiries mailbox monitored by the Quarantined Emails Enquiries team, which was part

of ANZ's security team. When MailMarshal was still operative, the employee could raise a request using ANZ's IT support ticketing system which would be actioned by the Quarantined Emails Enquiries team.

14. If the Quarantined Emails Enquiries team received an employee request to release an email, the email was reviewed and released if it was appropriate to do so. If the Quarantined Emails Enquiries team determined that it was not appropriate to release the email, it notified the employee of the reason why the email was quarantined and would not be released.

15. Although both inbound and outbound emails were monitored by email security systems during the Relevant Period, there were different rules for inbound and outbound emails. Inbound emails were prone to false positives (that is, they were prone to being quarantined when they did not contain prohibited language), including where part of a person's name matched a keyword. As a result, inbound email monitoring was subject to less stringent controls to ensure fewer false positives and a higher delivery rate of inbound emails. In practice, this meant that certain words, for example "shit", were omitted from the inbound email list of identified keyword terms but were included in the outbound email list of identified keyword terms.

16. Outbound email monitoring was more sensitive to prevent inappropriate content being sent by ANZ employees to external parties. As a result, outbound emails that contained potentially inappropriate content were more frequently quarantined than inbound emails. The reason for this approach was to ensure that ANZ employees received as many inbound emails as possible, even though the content might be inappropriate. For example, a customer complaint might contain strong language such as a swear word, but it was necessary for ANZ to receive the email so that the complaint could be addressed.

17. I regularly received queries from employees who had received an email that contained a word that was not an identified keyword term for inbound emails but was an identified keyword term for outbound emails. Often the offending word was buried deep in a chain of emails sent by someone from another organisation, so when the ANZ employee tried to reply to the email, it would then be quarantined by ANZ's email security systems. When that occurred, it was my practice, and the practice of others in my team, to advise the employee to search through the email chain and delete the offending word so that the email could then be sent without the inappropriate content.

18. As described above, MessageLabs and MailMarshal were the only email security systems in place during the Relevant Period to monitor and filter the content of emails. If an email was not identified and quarantined by MessageLabs or MailMarshal, the email

was not otherwise monitored for swear words and other inappropriate language and variations of them.

19. If an employee who was the sender or recipient of a quarantined email did not make a request for the email to be released, the quarantined email would not be reviewed. This meant that an employee could send an email that was full of profanities to an external person, which would then be quarantined without leaving ANZ's IT system. This approach was adopted due to the volume of inbound and outbound emails that were (and are) passing through ANZ's email security systems each day. It was not feasible for staff to manually review every quarantined email, and to carry out such a review in a timely way.

20. Although I can no longer recall or locate statistics relating to the number of quarantined emails during the Relevant Period, in preparing this affidavit I have obtained recent statistics of the number of inbound and outbound emails passing through ANZ's IT system which show the following:

    (a) During March 2023, there were 21,637,135 inbound emails received and 8,531,306 outbound emails sent. 727,655 of those emails were quarantined by ANZ's email security system;

    (b) During April 2023, there were 18,224,953 inbound emails received and 5,860,295 outbound emails sent. 373,820 of those emails were quarantined by ANZ's email security system; and

    (c) On 23 May 2023, there were 976,678 inbound emails sent and 285,527 outbound emails received. 94,762 of those emails were quarantined by ANZ's email security system.

21. Now produced, shown to me and marked '**DJM-1**' are screenshots of Splunk, an event monitoring and data aggregation platform used by ANZ, which were extracted by the Email Protection Squad from the platform, recording the above statistics.

CB 9546
ZNA.001.001.2784

22. In preparing this affidavit, I have also obtained historical statistics of the total number of emails received by ANZ's internal Microsoft Exchange email servers. This includes inbound (excluding quarantined or filtered emails), outbound and internal emails between ANZ staff passing through ANZ's IT system during specific months which show the following:

    (a) During March 2011 and April 2011, there were approximately 50.2 million and 41.3 million emails received and sent respectively; and

    (b) During March 2012 and April 2012, there were approximately 56.5 million and 51 million emails received and sent respectively.

23. Now produced, shown to me and marked '**DJM-2**' is an ANZ mail growth report which I retrieved from my email archive, which includes details of the number of emails sent and received (both internal and external to ANZ) for the period from 2009 to 2012, including the statistics outlined above. These reports were used during the Relevant Period for operational purposes to forecast ANZ disk space requirements.

CB 1030
ZNA.001.001.0090

Email monitoring of emails sent internally between employees at ANZ during the Relevant Period

24. ANZ's Australian email security systems did not have the capability to monitor emails for inappropriate content when those emails were sent between ANZ employees using their ANZ corporate email account (i.e. internal emails) during the Relevant Period. MessageLabs and MailMarshal both required an email to either enter or leave ANZ's IT system in order to be able to monitor the email for inappropriate content.

25. As a result, during the Relevant Period, ANZ employees could send internal emails to each other that contained inappropriate words and those emails would not be quarantined by ANZ's email security systems (as might have been the case if the ANZ employee used the word in an outbound email). By way of example, if during the Relevant Period an ANZ employee sent an internal email containing a crude joke or inappropriate content, we were reliant on someone raising a complaint or making a report about the email which may then lead to an investigation.

Storage and retrieval of emails during the Relevant Period

26. During the Relevant Period, ANZ used an enterprise information archive platform called Symantec Enterprise Vault (**Enterprise Vault**) to retain all emails sent and received by ANZ employees on their ANZ corporate email accounts. This included inbound, outbound and internal emails, except for inbound emails that were not received in the first place by an employee's corporate email account, including because they were quarantined by MailMarshal or MessageLabs.

27. At the start of the Relevant Period, emails were stored on Enterprise Vault for seven years. At some stage during 2014, the retention period increased to 10 years.

28. The retrieval of an employee's retained emails was typically prompted by an investigation by human resources, an employee complaint, a regulatory requirement or investigation or a Freedom of Information request. When the retrieval of an employee's retained emails was required, the procedure was for the relevant business area to submit a request, which was then reviewed, the search carried out and results exported. There were safeguards around this procedure to ensure that a request was made for a proper purpose and the business area was not asking for more records than was necessary for the purpose of the request.

29. Other than in the circumstances described above, during the Relevant Period, ANZ did not regularly or periodically review or audit emails retained on Enterprise Vault.

Automated emails received by Etienne during his employment

30. For the purposes of preparing this affidavit, I have been provided with extracts of four emails that were sent by the Applicant (**Etienne**) and provided to him as part of a disciplinary process which resulted in the termination of his employment (which are exhibited to the redacted affidavit of the Applicant affirmed on 21 December 2022 at pages 1599, 1607 and 1646). I did not have any involvement in the disciplinary process involving Etienne, the decision to terminate Etienne's employment or any other decisions relating to Etienne's employment.

CB 3602
ALEX.001.001.0966

31. Although ANZ had email security systems in place to monitor emails during the Relevant Period (which were as I describe above), the systems were not always effective and on occasions employees were able to send outbound emails that contained inappropriate language without those emails being quarantined by MailMarshal or MessageLabs.

32. For the purposes of preparing this affidavit, I have been provided with copies of six automated emails retained on Enterprise Vault during the Relevant Period that were sent to Etienne from the email address, alert@notification.messagelabs.com. Now produced, shown to me and marked '**DJM-3**' are copies of the automated emails dated 6 January 2012, 9 February 2012, 28 February 2012, 18 October 2012, 29 April 2013 and 24 August 2013, which have been redacted to mask the identity of each of the external email recipients in order to maintain the privacy of those other people, who are not party to these proceedings. The automated email contained a message in the following terms:

CB 1680
ZNA.001.001.0623

> *It is identified that this email contained inappropriate language (Example: swear words) which breaches the 'Use of Systems, Equipment and Information Policy'. It is important that you take appropriate care to ensure that any emails sent by you comply with ANZ policy. It is also everyone's obligation to protect ANZ's reputation…please contact quarantinedemailenquiries@anz.com for more information.*

33. I have been provided with a copy of an email retained on Enterprise Vault that indicates that Etienne contacted the Quarantined Emails Enquiries team on 9 February 2012 in relation to an email that he had attempted to send but had been quarantined. Etienne's email stated that:

> *CAn [sic] someone please explain this email , the sent mail did not contain any offensive language*

34. Now produced, shown to me and marked '**DJM-4**' is a copy of the email from Etienne to the Quarantined Emails Enquiries mailbox dated 9 February 2012, which has been redacted to mask the identity of the external email recipient in order to maintain the privacy of that other person, who is not party to these proceedings. CB 1699 ZNA.001.001.0642

35. The Quarantined Emails Enquiries team then responded to Etienne on the same date. The email stated that:

> *Etienne,*
> *Shite is in the email trail. This is the word that is required to be filtered.*
> *Please remove the word and resend this email.*
> *Regards,*
> *Liou*

36. Now produced, shown to me and marked '**DJM-5**' is a copy of the email from the Quarantined Emails Enquiries team to Etienne dated 9 February 2012, which has been redacted to mask the identity of the external email recipient in order to maintain the privacy of that other person, who is not party to these proceedings. CB 1700 ZNA.001.001.0643

Sworn by the deponent)
at Melbourne)
in Victoria)
on 17 November 2023)
Before me:)

[redacted]

Signature of deponent

[redacted]

Signature of witness

Name of witness: James David Wintle Sutherland

Qualification of witness: An Australian Legal Practitioner within the meaning of the *Legal Profession Uniform Law* (Victoria)

This document was sworn via audio-visual link. An electronic copy of this document and not the original has been used when completing the jurat requirements under section 27(1) of the *Oaths and Affirmations Act 2018* (Vic).

The requirements for witnessing by audio-visual link under section 12 of the *Electronic Transactions (Victoria) Act 2000* (Vic) have been met.