

Witness name: Dan O'Mahoney

Statement No: WITN11760100

Dated: 3 October 2024

THE POST OFFICE HORIZON IT INQUIRY

FIRST WITNESS STATEMENT OF DAN O'MAHONEY ON BEHALF OF POST OFFICE LIMITED IN THE POST OFFICE HORIZON IT INQUIRY

I, Dan O'Mahoney of 100 Wood Street, London, EC2V 7ER, will say as follows:

A. Introduction

- 1 I am Dan O'Mahoney, Inquiry Director at Post Office Limited ("**Post Office**"). This is my first Witness Statement to the Inquiry. I am giving this witness statement in a corporate capacity on behalf of Post Office, in response to the Rule 9 request dated 19 September 2024 ("**R9(62)**"). I am aware of the steps Post Office has taken to respond to this R9(62); as such, I am the appropriate person to give this witness statement on behalf of Post Office.

- 2 I have aimed to include within this witness statement evidence relating to R9(62) insofar as the relevant facts are within my own knowledge. The facts in this witness statement are true, complete and accurate to the best of my

knowledge and belief. Where my knowledge and belief, as set out in this witness statement, has been informed by another person or by documents that I have reviewed, I acknowledge that person or those documents. I have been assisted in preparing this witness statement by Burges Salmon LLP and Fieldfisher LLP (together "**BSFf**"), who act on behalf of Post Office in the Post Office Horizon IT Inquiry (the "**Inquiry**"). I have also been aided by Richard Crawley within Post Office's cyber department who has provided technical audit analysis required to respond to R9(62) in particular in (i) outlining the audit log processes at Appendix 1 and (ii) providing the underlying data analysed in devising the list contained in Appendix 2.

B. Methodology

- 3 R9(62) refers to the document titled 'Strictly Private and Confidential Investigation Report: Pineapple' (**POL00460000**) dated 1 September 2024 (the "**Report**") and requires that Post Office "*identifies every person within Post Office Limited who has received or accessed a copy of this document, including the dates on which those persons first received or accessed it*". The Report has a corresponding file name of '*Pineapple Investigation Outcome report Final 4924.pdf*'. The Inquiry has requested that Post Office identifies individuals within the business which have accessed or received a copy of the Report. Following analysis carried out by Post Office's cyber department, I understand that previous draft versions of the Report were received or accessed within Post Office on 2 September, two days prior to the circulation of the final Report. For completeness, I have also

included details at Appendix 2 of the individuals who have accessed or received copies of the following documents with a file name of:

- (a) *'Pineapple Investigation Outcome report Final 4924.docx'*
- (b) *'Pineapple Investigation Outcome report DRAFT.docx'*; and
- (c) *'Pineapple Investigation Outcome report DRAFT_NB comments.docx'*.

4 Post Office's cyber department have analysed the data in respect of the aforementioned drafts but have not located or seen actual copies of these drafts. I also have not seen copies of these individual drafts of the Report. As outlined in Appendix 2, I have only seen a final version of the Report.

5 Following the receipt of R9(62), Post Office checked its internal email records and confirmed that the following six individuals within Post Office had received a copy of the Report on 4 September 2024, circulated by Nicola Marriot:

- (a) Saf Ismail;
- (b) Elliot Jacobs;
- (c) Neil Brocklehurst;
- (d) Owen Woodley;
- (e) Karen McEwan; and
- (f) Myself (Dan O'Mahoney).

6 A list of the above individuals was provided to the Inquiry by email on Friday 20 September 2024 in advance of the filing of this witness statement. This email also acknowledged the additional 'technical searches' required to provide a

response to this R9(62). Such technical analysis forms the basis for the methodology in this statement.

- 7 Upon receipt of R9(62), Post Office engaged with members of its IT and cyber teams to extract and process the Report's audit data, using standard audit applications that are available across the Microsoft 365 proprietary application suite (together, the "**Audit Log Data**"). I understand that these audit processes are routine in the context of cyber security investigations which can also provide for analysis and oversight on document data and user activity. Audit Log Data provides an efficient means of compiling the required detail as to when, and by who, the Report is accessed, modified and disseminated within Post Office's electronic data universe. This Audit Log Data comprises the basis of the review methodology in responding to R9(62):

- (a) Microsoft Defender DeviceFileEvents Log – searched using the Microsoft Security portal. Search terms were limited to file names together with a date range parameter applied. Results are exported and searched across date limits.
- (b) Microsoft 365 Audit Log – searched using the Purview web interface targeting: Files, Folders or Sites across a search field with a confined search data parameter of 2024-08-20 to 2024-09-20. Results are exported and cross referenced as against DeviceFileEvents.
- (c) Microsoft Security Explorer - Mail-flow analysis – searched using the identified list of file name variants for the Report. For each variant, a

summary table of email metadata was export to Excel from the audit log data.

- 8 Details of the relative functionality and technical scope of the above audit logs are set out in Appendix 1 of this witness statement.
- 9 The Audit Log Data across the above logs was then extracted and assimilated into a consolidated spreadsheet setting out log entries for the Report and its draft versions.

C. Response

- 10 The Audit Log Data is consistent with and supports the initial investigations carried out by Post Office outlined at paragraph 5, above, as it identifies the six Post Office individuals who received a copy of the Report. This further audit analysis also identifies a number of additional individuals within Post Office that have also received or had access to the Report by way of the Audit Log Data. A list of all Post Office individuals who according to the Audit Log Data have had access to, or received a copy of, the Report is set out at Appendix 2 of this witness statement. This list sets out the individuals at Post Office that had access to or received a copy of the Report (or previous drafts) as at 12:00 on 20 September 2024 at the point in which the Audit Log Data was harvested. This document may have been accessed or received by additional individuals within Post Office between 20 September 2024 and the date of this statement; however, it has not been possible to undertake a rolling analysis or audit

following this date. Separately, the Audit Log Data is limited to only those activities within Post Office, and once data is sent to a non-Post Office recipient, there is no way to track or audit any subsequent document access or interactions. As such Post Office does not have sight of any wider dissemination of the Report outside of its own data universe.

- 11 Post Office has not produced the actual Audit Log Data generated as part of these investigations as such audit logs are technically complex and very large (with thousands of line items of data across multiple tabs of a spreadsheet); however, this has been retained should the Inquiry require it. Post Office has instead extracted and reviewed the Audit Log Data and has compiled a list of the individuals within Post Office that have received or accessed the Report and when.

Statement of Truth

I believe the content of this statement to be true.

GRO

Dan O'Mahoney

Date: **3 October 2024**

APPENDIX 1: AUDIT LOG SEARCHES UNDERTAKEN IN RESPONSE TO R9(62)

- 1 This appendix refers to the three audit logs that were interrogated and reviewed for the purposes of responding to R9(62). The following information has been provided to me by Richard Crawley of Post Office's cyber department who assisted in carrying out this technical analysis which informed the methodology and Audit Log Data to respond to Rule 9(62) and draft the consolidated list at Appendix 2.

Microsoft 365 Audit Log

- 2 Microsoft 365 Audit Logs (sometimes referred to as Purview Audit, Unified Event Log or Cloud App Security Log) provide for a centralised log of all activities recorded within Post Office's Microsoft 365 tenant which monitor and track changes all data held within online repositories, including to the Report. These audit logs are generated where a Post Office 365 account interacts with the Microsoft platform. This includes (i) human interactions such as where the Report is accessed, downloaded, modified, renamed or deleted; as well as (ii) background and automated processes, including OneDrive background synchronisation.
- 3 Post Office's cyber department also reviewed print event logs to assess whether the Report has been printed to a different document format, most commonly a hard copy print. No print events were identified to indicate that the Report had been printed to hardcopy or disseminated further.

Microsoft DeviceFileEvents Log

- 4 DeviceFileEvent log data represents auto-generated file system events and interactions recording on MS Windows devices such as user laptops, which includes at the point of creation, access and modification. DeviceFileEvents logs also provide for records such as where a document has been subject to a Microsoft Outlook mail attachment preview. DefineFileEvents are recorded from the laptop device but are stored online and are searchable with the 365 Audit data.

Microsoft Security Explorer - Mail-flow analysis

- 5 Microsoft mail-flow log data provides a detailed, 30-day rolling record to capture and track all actions and metadata across email activity. Technical investigations for all cyber security incident matters can be carried out to search across email attachments providing for detailed email mail flow tracking analysis.

**APPENDIX 2: INDIVIDUALS WITHIN POST OFFICE LIMITED WHO RECEIVED
OR ACCESSED A COPY OF THE REPORT**

Key

	Mail-Flow Analysis log
	DeviceFileEvent log

**1. Pineapple Investigation Outcome report Final 4924.pdf (.docx)
(POL00460000)**

Name	Email Address	Date first received/accessed
Nicola Marriott	nicola.marriott@postoffice.co.uk GRO	04/09/2024 10:39 ¹
Saf Ismail	saf.ismail@postoffice.co.uk GRO	04/09/2024 10:39
Elliot Jacobs	elliot.jacobs@postoffice.co.uk GRO	04/09/2024 10:39
Neil Brocklehurst	neil.brocklehurst@postoffice.co.uk GRO	04/09/2024 10:45
Karen McEwan	karen.mcewan@postoffice.co.uk GRO	04/09/2024 10:45
Owen Woodley	owen.woodley@postoffice.co.uk GRO	04/09/2024 10:45
Dan O'Mahoney ²	dan.o'mahoney@postoffice.co.uk GRO	04/09/2024 10:51
Rachael Wheeler	rachael.wheeler@postoffice.co.uk GRO	04/09/2024 10:51
Andrea Beveney ³	andrea.beveney@postoffice.co.uk GRO	12/09/2024 13:41
Nick Read	nick.read@postoffice.co.uk GRO	13/09/2024 08:35

¹ This date represents the date in which Nicola Marriott first shared the final version of the Report with individuals within Post Office.

² A copy of the Report was circulated to Dan O'Mahoney in his capacity within Post Office's Inquiry legal team only.

³ A copy of the Report was circulated to Andrea Beveney in her capacity within Post Office's Inquiry legal team only.

Lyn Daniels ⁴	lyn.daniels@GRO	13/09/2024 12:09
Chrysanthy Pispinis	chrysanthy.pispinis@GRO	17/09/2024 14:46
Amanda Burton	amanda.burton@GRO	20/09/2024 09:30

2. Pineapple Investigation Outcome report DRAFT.docx⁵

Name	Email Address	Date first received/accessed
Nicola Marriott	nicola.marriott@GRO	23/08/2024 12:30 ⁶
Karen McEwan	karen.mcewan@GRO	02/09/2024 07:47
Neil Brocklehurst	neil.brocklehurst@GRO	02/09/2024 07:47
Owen Woodley	owen.woodley@GRO	02/09/2024 07:47
Phillipa Hankin	phillipa.hankin@GRO	02/09/2024 09:32
Tim Perkins	tim.perkins@GRO	02/09/2024 13:31
Tracy Cox	tracey.cox@GRO	10/09/2024 18:10

3. Pineapple Investigation Outcome report DRAFT_NB comments.docx

Name	Email Address	Date first received/accessed
Nicola Marriott	nicola.marriott@GRO	04/09/2024 09:28

⁴ Lyn Daniels is the Personal Assistant to Karen McEwan – Lyn Daniels accessed the document by way of an Outlook preview function which provided for a DeviceFileEvent log entry. This may have happened because of Ms Daniels having a shared inbox function by virtue of her role as Karen McEwan's PA but cannot confirm this on the basis of the audit. Following reviews across the Audit Log Data, Ms Daniels did not directly access or download the Report in full.

⁵ Previously titled "Pineapple Investigation Outcome report.docx"

⁶ Nicola Marriott was the document author of the Report. This represents the first instance in which a DeviceFileEvent was registered in which Nicola Marriott accessed and modified this draft version of the Report after 26 August 2024.

Karen McEwan	karen.mcewan	GRO	04/09/2024 09:28
Neil Brocklehurst	neil.brocklehurst	GRO	04/09/2024 09:28
Owen Woodley	owen.woodley	GRO	04/09/2024 09:28

Index to the First Witness Statement of Dan O'Mahoney

No.	URN	Document Description	Control Number
1.	POL00460000	Strictly Private and Confidential Investigation Report: Pineapple	POL-BSFF-WITN-055- 0000001