POL00029049

Deloitte.

Deloitte LLP
2 New Street Square
London
EC4A 3BZ

Phone: GRO
Fax: +
www.deloitte.co.uk

markwestbrook GRO

# Memo

**Date:** 3 September 2018

**To:** Post Office Limited

**From:** Deloitte LLP

**CC:**

**Subject** Project Bramble – Document Review

Private and Confidential – Subject to legal privilege.

**Overview:**

We have reviewed the 97 documents requested for any content which contradicts the Project Bramble report issued on 02/02/2018 and any content that could pose an IT security risk to the Horizon system either by divulging security sensitive information or highlighting weaknesses in IT Security controls. We have also noted any content of the documents which is of specific note. Our high level conclusions are below, and the detailed output on a document by document basis is in the embedded Excel file. In summary, almost nothing we have read in the 97 documents reviewed contradicts the Bramble report dated 02/02/2018 (the notable possible exception being that described in document 'ADDES065', page 30, where a long term exception to the principle that each transaction on Horizon, or Riposte as it then was, has a unique identifier is discussed – we recommend further investigation of this point).

The documents do provide a number of details such as account names, filenames, database table information, and underlying data within the systems, which could compromise security, and Post Office will need to consider the implications from these.

**Document classification and focus:**

Broadly, with exceptions, you could classify the documents reviewed to date as:

- Documents about data flows, including reconciliation controls;
- Lessons learned documents (which highlight everything which has gone wrong/caused challenges during project delivery, from both a technical and project delivery perspective and learnings that can be taken into future projects);
- End user guidance documents; and
- Post incident reports (detailing incidents which have caused some downtime / post office issues) (ranging from one branch to thousands), for example: 'CSREP198' and 'CSREP189'.



The focus of the documents does not have much overlap with the scope of our Project Bramble work for Post Office Limited to date.

POL00029049

Deloitte.

- Many of the documents describe historical controls around the Horizon system, with many dating back to the 1990's. They describe processes and controls, which in many cases are no longer present, our work to date has focused largely on the current control environment;

- Much of the interface information relates to the infrastructure around POLSAP, TPS, APS, DRS and Credence – which has been largely outside of our scope, (rather than the 'master' data flow from Counter to the Audit Store which our work to date has been focused on). Previously this has been discussed and deemed surplus to requirements as reliance is placed on the transaction acknowledgement process for the acceptance of data from third parties (and any other data source that is not the counter);

- Specifically a number of documents detail the reconciliations done between various data sources / flows including third party data. There is not much detail on the investigatory follow up process / controls in place to rectify any errors / error reporting;

- Of particular note is document, 'NBHLD004' - The DRS reconciles data from the counter which flows through Horizon infrastructure to third party data. We have done no work over this system. The diagram at the very back of our Sparrow report could be embellished with further work over DRS and the other infrastructure noted in the above bullet; and

- There is an extra interface to the data flow pre BRDB, which we have not looked at, involving data being sent to third parties for validation before it is sent from the Counter to BAL and then onwards to the BRDB (essentially a 'handshake' with third parties to check sufficient funds for transactions to be processed). This is an enhancement to our current understanding, and does not contradict the conclusions of the Sparrow report.

**Summary of Security:**

A number of the documents contained 'security sensitive' information:

- A significant proportion (>50%) of the documents contain high levels of detail on batch jobs, SQL code, account names, file locations, naming conventions, URLs, PCI relevant data and system storage limits which could pose a security risk if made public. Some contain risky information such as IP addresses and there is even an embedded PEN test report highlighting specific weaknesses / vulnerabilities on certain Horizon architecture. There is no document identifying how POL responded to the PEN test findings; and

- Some personal information (name, e-mail) of Fujitsu staff are also contained within the documents.

**Other points of note:**

Some other points of note arising from the document reviews:

- Some documents are 'forward looking' – and are written in such a way to indicate there are issues (or imperfections) with the current system as it is, hence justifying the need for future changes (for example: 'DESAPPDPR3381');

- A number of documents are 'in review' and have tracked changes and/or embedded comments, some documents have the watermark 'withdrawn';

POL00029049

Deloitte.

- A number of documents are 'commercial in confidence' or 'Fujitsu restricted';
- For the documents which are 'Post incident reports', some include this text "TO AVOID ANY CONFUSION IT HAS BEEN DECIDED THAT POST INCIDENT REPORTS ARE TO BE INTERNAL FUJITSU DOCUMENTS & NOT TO BE SENT TO ATOS OR POL"; and
- At least one of the documents contains an NDA (Non-Disclosure Agreement) which will need considering before release. (TDARC026).

**Limitations**

We have reviewed the document explicitly against the scope points listed in the statement of work. We have highlighted at a document level where security sensitive information is divulged, we have not highlighted every instance of security sensitive information in the document. Further where there is security sensitive information such as code, pseudocode, batch schedules and other table data, we have not reviewed these in detail and are not providing a view on the logic contained within this code.

**Documents of Potential Interest:**

Based upon our review and understanding of your purpose we have highlighted the following documents as those which you might find of most interest for early review. However, set out in the embedded spreadsheet is an analysis of all the documents provided which should be evaluated in full by Post Office.

- DEVAPPSPG0028 (DRS Host Support Guide):
    - Covers the DRS system which we have not looked at before;
    - Contains an embedded review comment querying the factual accuracy of a section (7.19.2); and
    - Indicates that it is not advised to run a certain process twice, but doesn't state the impact (7.4.2).
- NBHLD003 (DRS Host High Level Design)
    - 5.3.2.2 implies that at a previous point in time the Data Reconciliation Service (DRS) could become out of sync and not reconcile with TPS (Transaction Processing Service) which could imply data deficiencies which could cause SPM detriment. This is also discussed in more detail in section 5.3.4.1.3;
    - Page 36 - technical limitations are highlighted and a work-around is detailed which could be an indicator of higher coding risk;
    - 5.3.5.1.2.3 - historical process is detailed which indicates a risk of data errors requiring manual intervention to rectify; and
    - Page 106 - ''Where the main store reaches an error state, these states are reported in the DRS Reconciliation reports and can be viewed using the DRS Workstation. Once discrepancies have been reconciled manually, either internally or with the Financial Institution, the status is manually set to F99 (Final State) so that they are no longer shown as outstanding.'' - This sounds like a key control, which is manual, and has not previously been brought to our

POL00029049

Deloitte.

attention. POL should consider the evidence they have to support this control. (This sentence also implies the 3rd party performs some of the reconciliations).

- ADDES065 (High Level Design Specification for Network Banking Agents):
    - Page 30 - details that the Horizon_Txn_Num is not guaranteed to be unique over a long period of time (citing that they will be re-used following the 're-rollout of an outlet');
    - Document refers to Riposte (dated 30/04/2004) and highlights a number of areas of potential concern for the case;
    - Page 24 - states that there are instances whereby messages generated by the counter will not be transferred centrally where network failures occur;
    - 5.1.4.6: ''It is expected that normally up to 2% of [R] messages will result in a [C0] being generated, so the workload on average will be up to 2% of that for the NBS Authorisation Agent. However following a failure of an Agent, a Correspondence Server or the NBE, then there could be peaks where 100% of [R]s will result in a [C0] being generated''; and
    - Page 55 - details a 'throttle' which controls the number of messages an agent sends is detailed, however "In practice, this throttle was never implemented by development." This implies that potentially (subject to further technical understanding) data could drop out should this limit be breached.
- DESAPPDPR3381 (ATM Transaction Simplification):
    - Document is in draft status and 'forward looking' to 'describe changes required for the 'ATM Transaction Simplification project';
    - 1.1 - "Post Office have identified that they have a problem with the management of ATM cash stock." – then provides detail of what the associated problems are;
    - 1.1.1 - "The history of the current solution is not known and the only documentation is in the attached ATM Operating Instructions." - The attached operating instructions (embedded in document) contains a paragraph on page 10 which details that if a branch operates after 4.30pm then specific actions need to be taken the following day to ensure correct treatment. The implications of failing to do this are not made clear;
    - 'ATM Operating Instructions' are embedded in this document (Section 1.1.1) – this in itself is a 40 page document;
    - The embedded 'ATM Operating Instructions' contains a lot of detail on retracts;
    - The embedded 'ATM operating Instructions' does not contain any information on how to contact POL to query any figures on the ATM reports / detail the process for flagging potential errors / investigations;
    - In section 3.3.1 of the embedded 'ATM Operating Instructions' it is stated that if 2 retracts occur the ATM will go out of service and can only be used again once retracted notes are removed. Further this can only be done once the Post Office is secure (i.e. out of hours);
    - In section 3.4 of the embedded 'ATM Operating Instructions' it is stated that "You do not need to make a physical count of the cash contained in the ATM in order to complete the

POL00029049

Deloitte.

declaration." This could be seen to be inducing SPMs to declare a value without the need to check it for accuracy;

- In section 3.4.3 of the embedded 'ATM Operating Instructions' (and throughout the rest of the document) the process for making a cash declaration is outlined. It is very manual with multiple steps. Manual, complex processes are by their nature more prone to fraud and error;
- In section 3.4. of the embedded 'ATM Operating Instructions' cash shortages are inferred to be unlikely and not expected / permissible. Indicating an investigation will follow should a cash shortage be detected;
- In section 6.1 of the embedded 'ATM Operating Instructions' the final bullet tells an SPM not to give cash to customers in event of a retract, or they will have to make good the loss. In reality with irate/challenging customers this may prove difficult; and
- In section 7 FAQ of the embedded 'ATM Operating Instructions' one of the questions is, 'Why do i have a cash shortage on my ATM balance?' - the answer infers the only reason why this could be is that the SPM has made a counting / calculation error. If retract fraud occurs this would leave a shortage however the answer does not state this. It is also likely that there are other possible reasons for a shortfall to exist.

- SVMSDMPRO0012 (Reconciliation and Incident Management Joint Working Document):
  - This is a document which provides an overall summary of banking reconciliations and associated data flows (Page 11 for example and the diagram on page 12). A number of controls / data flows are listed here in detail which could be looked at further. No work has been done over this to date; and
  - 1.1 - "It is acknowledged that not all system faults will lead to corrective action as this is generally done on a contractual and/or cost benefit basis." – this statement could be of interest to the current legal proceedings.
- DESAPPHLD2255 (HNG-X Counter Audit Event IDS):
  - Excel sheet has comments embedded indicating POL & FJ do not work well together "(I'm not sure what Event Report mappings is - I think it is something POL did internally so I don't want to lose it)";
  - The Event Report mappings tab contains numerous notes from POL and Fujitsu, some of which indicate the audit events either do not work correctly or are not required; and
  - Some of the events highlight that (if triggered) the system would not have been operated as expected, and therefore could raise questions over the system.
- PMREP010 (Lessons Learnt from the S60 Release):
  - This document is an example of one of the lessons learnt documents which highlight errors in past projects / processes;
  - Document highlights communication challenges between POL and Fujitsu which may be of interest to the legal proceedings. One of the issues raised is around failing to capture and agree business requirements properly; and
  - Page 32 alludes to errors in the data migration for the S60 release.

POL00029049

Deloitte.

- CSREN032 (S80 Release Note - Deferred Peaks List – Counter):
    - This document includes the list of bugs which went out with S80 of Horizon. Some of these bugs (for example see top of page 8), could be construed to indicate risk of erroneous data which could result in sub-postmaster detriment. PC0116293 highlights a bug in the alerting of subpostmasters to SU imbalances. PC0116581 highlights a bug relating to misleading information on online services being unavailable when a TC is issued. PC0117852, and PC0119894 also outline shortcomings in the system which could result in subpostmaster confusion. PC0120245 could indicate potential risk to SPMs as well. PC0120471 highlights errors not being written to the event log. PC0120509 highlights. PC0121925 is indicative of an issue which could lead to subpostmaster detriment.
- SDREQ001 (Reconciliation Requirements Analysis):
    - Very old document, dating from 1998. The document hints fairly strongly that reconciliation was considered fairly late on during the requirements consideration for release NR2, which may be of interest to the legal proceedings;
    - Highlights throughout that at the time the document was written, there were plenty of exceptions compared to requirements with the reconciliation controls with external parties related to the Horizon (then called Pathway) system; and
    - Section 5 contains a list of requirements which POL/Fujitsu should be doing around reconciliation with the delivery of NR2, which may be of interest to the legal proceedings.
- IAREQ005 (Network Banking Internal Audit Requirements):
    - This document contains details of challenges with the Audit server given the move to NWB and contains evidence of historical breaks in the audit trail due to simultaneous downtime at both data centres and a lost tape.
- CSREN029 (S75 Release Note - Deferred Peaks List LINK Cutover (R1)):
    - This document includes the list of bugs which went out with release S75 of Horizon. Some of these bugs (for example see top of page 8), could be construed to indicate risk of erroneous data which could result in sub-postmaster detriment. PC111263 PC111457, PC111523 and PC109777 are of particular interest the latter (PC109777) because of its mention of SSC users (remote access to branches).
- EATRP007 (Impact Release 3 Transaction Correction Application Test Report):
    - This is a brief document reporting on transaction correction functionality to the branch counter. The key point within the document is that a number of exceptions were raised by testing (but are not detailed within the document), which might undermine confidence in the correct operation of transaction corrections.

Please see the accompanying excel for a full view of notes made during the document reviews.

POL00029049

Deloitte.