



HORIZON DATA CHANGES PROCESS WORK INSTRUCTION
FUJITSU RESTRICTED (COMMERCIAL IN
CONFIDENCE)



Document Title: HORIZON DATA CHANGES PROCESS WORK INSTRUCTION

Document Reference: SVM/SDM/PRO/4293

Release: Not applicable

Abstract: Fujitsu internal work instructions stating the scenarios under which Fujitsu specialist support staff make changes to Live data to maintain the effective operation of HNG-X.

Document Status: APPROVED

Author & Dept: Sandie Bothick & Steven Browell

External Distribution: N/A

Information Classification: See section 0.9

Approval Authorities:

Name	Role	
Steven Browell	Management Consultant & CISO	See Dimensions for record
Steve Bansal	Senior Service Delivery Manager	See Dimensions for record



HORIZON DATA CHANGES PROCESS WORK INSTRUCTION
FUJITSU RESTRICTED (COMMERCIAL IN
CONFIDENCE)



0 Document Control

0.1 Table of Contents

0	DOCUMENT CONTROL.....	2
0.1	Table of Contents.....	2
0.2	Document History.....	3
0.3	Review Details.....	3
0.4	Associated Documents (Internal & External).....	4
0.5	Abbreviations.....	4
0.6	Glossary.....	5
0.7	Changes Expected.....	5
0.8	Accuracy.....	5
0.9	Information Classification.....	5
1	PURPOSE & SCOPE.....	6
2	TYPES OF HORIZON DATA CHANGE.....	6
3	CHANGE MANAGEMENT.....	6
4	DEFINED SERVICE OBLIGATIONS.....	6
5	HORIZON DATA CHANGE PROCESS.....	7
5.1	Overview.....	7
5.2	Investigation Stage – the Incident.....	8
5.3	Taking the Action Required.....	8
5.3.1	Process Overview.....	8
5.3.2	Obtain POL Approval.....	8
5.3.3	Obtain Fujitsu Approval.....	9
5.3.4	Grant Additional Elevated Privileges - if required.....	10
5.3.4.1	Reporting on Granting of Additional Temporary Elevated Privileges.....	11
5.3.5	Make the data change.....	11
5.3.6	End the process – closing the Incident.....	11
5.4	Reporting on Horizon Data Changes.....	11
6	CONTINUOUS IMPROVEMENT.....	11
	APPENDIX A – POL AD-HOC FORM EXAMPLE.....	12
	APPENDIX B – EVIDENCE EXAMPLES.....	13
B.1	SQL Evidence.....	13
B.2	File Removal Evidence.....	13



HORIZON DATA CHANGES PROCESS WORK INSTRUCTION

FUJITSU RESTRICTED (COMMERCIAL IN CONFIDENCE)



0.2 Document History

Only integer versions are authorised for development.

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change CP, CCN or PEAK Reference
0.1	28/06/2021	Initial Draft	Include if known
0.2	29/06/2021	Reorganised document structure and removed some unnecessary sections	
0.3	13-May-2022	Revised in response to review comments	
0.4	01 July 2022	Revised in response to review comments	
0.5	07 July 2022	Improved structure of content	
0.6	08 July 2022	Revisions after feedback	
0.7	15 July 2022	Further revisions after feedback from SecOps	
0.8	20 July 2022	Further revisions from MAC and SSC	
0.9	27 July 2022	Further revisions from feedback from SecOps, MAC and SSC. Added Change Management as a scenario. Changed APPSUP to "elevated privileges" as a better definition – and in readiness for inclusion of Post Office Cloud processes into this document. Expanded acronyms on first use	
1.0	01- Aug 2022	Approval version	
1.1	01-Aug-2023	Change to "Optional Review" list. Change to "Issued for Information" list. Update to "Abbreviations" list. Update to section 5.3.4	
1.2	10-Aug-2023	Change "script" to "command" in section 5.3.4. Append "(or deputy if unavailable)" to Fujitsu approval named role, section 5.3.3.	
2.0	11-Aug-2023	Approval version	

0.3 Review Details

Review Comments by:	
Review Comments to:	Steven.browell@GRO PostOfficeAccountDocumentManagement@GRO
Mandatory Review	
Role	Name
Management Consultant & CISO	Steven Browell
Senior Service Delivery Manager	Steve Bansal
SSC Manager	Adam Woodley; GMBXSSCDutyManager@GRO
MAC and OBC Service Delivery Manager	Sandie Bothick
Information Security Manager (Security Governance)	Chris Stevens
Information Security Manager (Security Operations)	Farzin Denbali
UNIX Team	PostOfficeAccountUNIXTeam@GRO
Optional Review	
Role	Name



HORIZON DATA CHANGES PROCESS WORK INSTRUCTION

FUJITSU RESTRICTED (COMMERCIAL IN CONFIDENCE)



MAC and OBC Service Control	Paul Elmes
MAC and OBC Service Control	Simon Cutmore
MAC and OBC Service Control	Hamid Abdul
MAC and OBC Service Control	Emma Millman
MAC and OBC Service Control	Jacqueline Wilcock
Security Analyst	Jack Steptoe
Security Analyst	Beverly Brown
Security Analyst	Ifran Khan
Security Analyst	Andy Dunks
Problem, Defect & Quality Manager	Matthew Hatch
Document Manager	Matthew Lenton

(*) = Reviewers that returned comments

Issued for Information – Please restrict this distribution list to a minimum	
Position/Role	Name
POADM	PostOfficeAccountDutyManager@ GRO
MAC Team	mac.uk@ GRO
POA SecOps	CSPOA.Security@ GRO

0.4 Associated Documents (Internal & External)

References should normally refer to the latest approved version in Dimensions; only refer to a specific version if necessary.

Reference	Version	Date	Title	Source
PGM/DCM/TEM/0001 (DO NOT REMOVE)	See note above	See note above	POA Generic Document Template	Dimensions
PGM/DCM/ION/0001 (DO NOT REMOVE)			POA Document Reviewers/Approvers Role Matrix	Dimensions

0.5 Abbreviations

Abbreviation	Definition
APOP	Automated Payment Out-Pay
APPSUP	Application Support – an Oracle database role that provides elevated privileges
CCD	Contract-controlled document
CSPOA	Cyber Security Post Office Account
GUI	Graphical User Interface
HDC	Horizon Data Change
MAC	Major Account Controller
MID	Merchant Identifier
MSAD	Microsoft Active Directory
NWH	Normal Working Hours (09:00 to 17:30 Monday to Thursday and 09:00 to 17:00 Friday – UK time - excluding UK Bank Holidays)



HORIZON DATA CHANGES PROCESS WORK INSTRUCTION

FUJITSU RESTRICTED (COMMERCIAL IN
CONFIDENCE)

OBC	Operational Branch Change
OOH	Out Of Hours (times outside of NWH)
POC	Post Office Cloud
PODG	Post Office Data Gateway
POL	Post Office Limited
RDMC	Reference Data Management Centre
SQL	Structured Query Language
TID	Terminal Identifier

0.6 Glossary

Term	Definition
TfSNow	Fujitsu service management toolset
Bonded	A developed feature of the Fujitsu TfSNow service management toolset and the POL ServiceNow service management toolset that allows an Incident to be linked allowing defined updates to replicate in both directions

0.7 Changes Expected

Changes
This document relates to live data changes in Belfast and will need to be updated to include Post Office Cloud (POC) once POL and Fujitsu processes are defined.
Removal of Clear Failed Recoveries as a Defined Service Obligation when Release 72.20 is deployed.

0.8 Accuracy

Fujitsu Services endeavours to ensure that the information contained in this document is correct but, whilst every effort is made to ensure the accuracy of such information, it accepts no liability for any loss (however caused) sustained as a result of any error or omission in the same.

0.9 Information Classification

The author has assessed the information in this document for risk of disclosure and has assigned an information classification of FUJITSU RESTRICTED (COMMERCIAL IN CONFIDENCE).



HORIZON DATA CHANGES PROCESS WORK INSTRUCTION

FUJITSU RESTRICTED (COMMERCIAL IN CONFIDENCE)



1 Purpose & Scope

This document describes the process Fujitsu will follow when making data changes to the Live HNG-X System in Belfast. It includes the three scenarios that can apply: Change Management; Defined Service Obligations; and the Horizon Data Change Process.

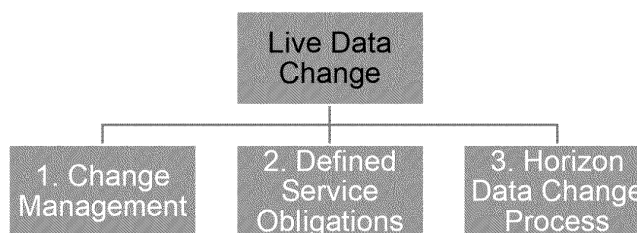
This document states the actions required, and the local work instructions used, by the teams to perform the necessary Horizon Data Change Process tasks. Each action clearly states the involvement of Post Office Limited (POL) in the process.

NOTE: Out of Hours (OOH) will follow the standard Post Office Account (POA) OOH processes.

2 Types of Horizon Data Change

The following are situations that mean that Fujitsu needs to make changes to data in the Live HNG-X System in Belfast:

1. **Change Management** – typically operational or project changes that follow the agreed POA & POL Change Management processes and approvals
2. **Defined Service Obligations** – processes that are defined in contract-controlled documents that require the intervention of Fujitsu specialist support staff. POL pre-approval is not required
3. **Horizon Data Change Process** – all other scenarios not covered under Defined Service Obligations. All of these require explicit POL pre-approval, and, in some cases, this will include a requirement for Fujitsu specialist support staff to be granted temporary additional elevated privileges (sometimes known as the APPSUP role) to be able to take the action required



These are described below.

3 Change Management

Changes may be submitted following the defined change management process on POA that require Live data to be changed. This should be described within the change description and approved by POA and POL as part of the standard approval procedures and using the agreed service management toolsets.

4 Defined Service Obligations

There are several defined service obligations held within agreed contract-controlled documents (CCDs) that require Fujitsu to make changes to data in the Live HNG-X System in Belfast. These are shown below with a summary description. The relevant Fujitsu specialist support staff always have the necessary privileges to perform these actions. The involvement of POL in each is stated:

1. Clear Failed Recoveries (script)



HORIZON DATA CHANGES PROCESS WORK INSTRUCTION

FUJITSU RESTRICTED (COMMERCIAL IN
CONFIDENCE)

- Part of the Fujitsu Reconciliation Service (SVM/SDM/SD/0015 & SVM/SDM/SD/0020). The Fujitsu Reconciliation Team raise Peak tasks for anomalies identified which then leads to the MAC team to raise a Fujitsu Change for SSC. Once the Change is approved internally by Fujitsu, the SSC run the required script. This happens frequently.
- 2. Clear Automated Payment (AP) Exceptions (GUI)**
 - Part of the Fujitsu Reconciliation Service (SVM/SDM/SD/0015 & SVM/SDM/SD/0020). The Fujitsu Reconciliation Team raise Peaks for anomalies identified which then leads to the MAC team to raise a Fujitsu Change for SSC. Once the Change is approved internally by Fujitsu, the SSC use the web GUI. This happens frequently.
- 3. Generate Reference Data / Integrity checks / Progression to Live**
 - Part of the Fujitsu Reference Data Management Service (SVM/SDM/SD/0013 & CS/PRD/058). POL Data Services raise Reference Data requests via the email gateway PEAK@GRO which generates a Peak task. Requests are only accepted from specific POL source email addresses. Fujitsu generate data for POL as per its request and then move the generated data into a specific directory. The data is then loaded to the live database using the Fujitsu RDMC GUI. Changes are made via tooling to the RDMC database.
- 4. Message Broadcast Service (MBS) progression to Live**
 - Part of the Fujitsu Message Broadcast Service (SVM/SDM/SD/0018). MBS files are submitted by POL to a Fujitsu group mailbox PostOfficeAccount.RefDataTeam@GRO. Requests are only accepted from specific POL source email addresses. The emails are automatically delivered to Live. There is no user involvement unless faults occur – typically in the POL data submitted.
- 5. PODG (OBC19) / Progression to Live**
 - Part of the Fujitsu PODG OBC19 service within the Data Centre Operations Service – Annex A (SVM/SDM/SD/0003). POL submit OBC19 forms to Fujitsu by email. Requests are only accepted from specific POL source email addresses. Fujitsu raise TfSNow Changes for the Fujitsu teams to perform the required actions. Changes are made via tooling to generate new XML configuration files.
- 6. Track & Trace Monthly Despatch Report Cut-off**
 - Part of CCN1627 and included in the Third Line Support Service (SVM/SDM/SD/0004). Post Office have an ongoing issue relating to subpostmasters not cutting off their Track and Trace (T&T) reports (formally known as Office Daily Postal Services Despatch Report) correctly. Fujitsu Service's 3rd Line support team perform a manual check each month to identify outstanding T&T despatch reports and manually remove all records above the 1500 threshold.

5 Horizon Data Change Process

5.1 Overview

The Horizon Data Change Process applies to all scenarios where changes are needed to data in the Live HNG-X System in Belfast that are not stated in the Defined Service Obligations.

This process requires that POL pre-approve the actions Fujitsu need to take and that POL are provided with evidence of the actions Fujitsu took. The process is managed using the service management toolsets so that an audit trail is created and retained.

The Horizon Data Change Process may require Fujitsu specialist support staff to be granted additional temporary elevated privileges in order to be able to perform the actions required.

There can be a variety of reasons why a data change is needed to the Live HNG-X data to resolve an Incident. Any action to effect a change to live HNG-X data must be approved by POL before the action is taken.

The following are example scenarios under which this Horizon Data Change Process could apply:

1. Assisted Branch Rollover.
2. Modifying or deleting files on a back-end system.



HORIZON DATA CHANGES PROCESS WORK INSTRUCTION

FUJITSU RESTRICTED (COMMERCIAL IN
CONFIDENCE)

3. Clear Branch Rollover lock (Deleted user/Deleted Kiosk).
4. Deletion of Orphaned User Sessions.
5. Clear APOP Exceptions.
6. Merchant Identifier (MID) / Terminal Identifier (TID) corrections.

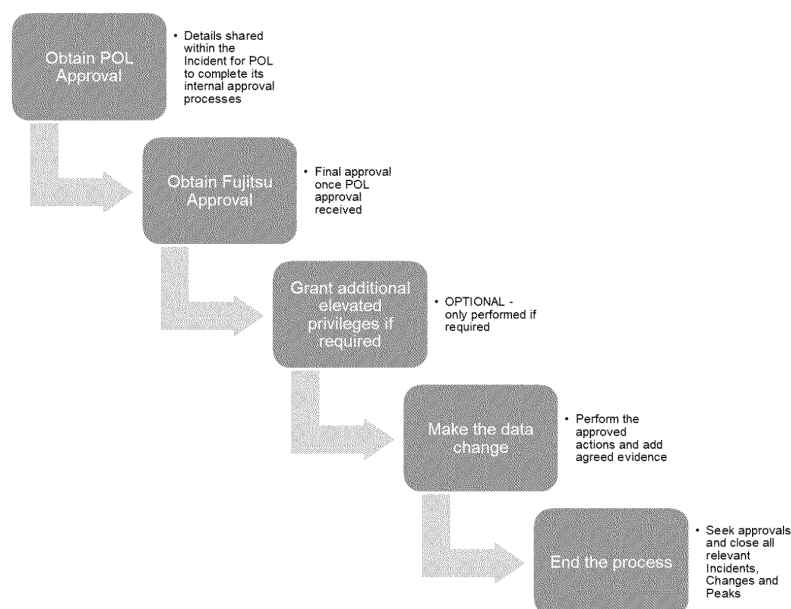
5.2 Investigation Stage – the Incident

The process starts with an Incident being logged in TfsNow, raised by either POL or Fujitsu. The Incident must be a bonded Incident. Fujitsu will investigate the Incident and will supply POL with options and suggested recommendations to resolve the issue. If additional temporary elevated privileges are required to be able to make data changes to the live HNG-X System in Belfast to resolve the Incident, then this will also be stated within the Incident update that POL will see.

5.3 Taking the Action Required

5.3.1 Process Overview

If the outcome of the Incident investigation is that a data change is needed to the live HNG-X System in Belfast, then the following process applies:



5.3.2 Obtain POL Approval

To request POL approval, Fujitsu will update the bonded Incident with the following information:

1. What action needs to be taken.
2. If applicable, Fujitsu will propose a timeframe either at this stage or later in the process. Otherwise, POL will provide this as part of their approved response.
3. What steps need to be taken (a plan if required).
4. What risks should be understood (if action is taken or action is not taken).
5. POL will then need to raise the POL Ad-hoc form using the information provided in the Incident and gain the required POL approvals (see Appendix A for an example POL Ad-hoc form). Fujitsu is not involved in the POL approval process and only requires a final confirmation and permission to proceed.



HORIZON DATA CHANGES PROCESS WORK INSTRUCTION

FUJITSU RESTRICTED (COMMERCIAL IN
CONFIDENCE)

6. POL will update the Incident to notify Fujitsu that approval has been granted with the approvals and POL Ad-hoc form attached to the Incident as evidence.
7. Fujitsu MAC team will check the POL Ad-hoc form matches the information Fujitsu provided in the Incident to ensure the approval matches the action Fujitsu need to take. If the POL Ad-hoc form does not match the information Fujitsu provided in the Incident, then the approval from POL will not be considered appropriate and the request will be rejected, and POL will need to either amend the POL Ad-hoc form or a new Incident will need to be raised.

NOTE: POL decide the communication messages and involvement actions with subpostmasters.

5.3.3 Obtain Fujitsu Approval

Once POL Approval has been obtained a final level of approval is needed by Fujitsu as changes could have been made by POL to the proposed approach or additional information could have been added by POL as part of its approval process.

1. If additional temporary elevated privileges are not required:
 - a. Fujitsu MAC team will email the Fujitsu Senior Service Delivery Manager (or deputy if unavailable) for approval.
 - b. If Fujitsu service management are satisfied with the details sent to them then they will confirm via email and the process will continue.
 - c. If Fujitsu service management are not satisfied with any of the details, then they will confirm via email and the process will go back to the Investigation stage for alternative options to be considered.
 - d. Fujitsu MAC will add the Fujitsu service management response to the TfSNow Incident.
2. If additional temporary elevated privileges are required:
 - a. The Fujitsu MAC team will email the Fujitsu Senior Service Delivery Manager (or deputy if unavailable) for approval to proceed and copy CSPOA Security for awareness. MAC team will include the CSPOA Template in the email:

Does this work require additional temporary elevated privileges from SecOps	Yes/No
When does this work need to occur	<<NWH/OOH>>
Time of work	dd/mm/ccyy hh:mm
Duration of time allowing completion of work	<<Duration>>

- b. If Fujitsu service management are satisfied with the details sent to them then they will confirm via email and the process will continue.
 - c. If Fujitsu service management are not satisfied with any of the details, then they will confirm via email and the process will go back to the Investigation stage for alternative options to be considered.
 - d. Fujitsu MAC will add the Fujitsu service management response to the TfSNow Incident.
3. If Fujitsu approval has been granted:
 - a. Fujitsu MAC team will raise a Change for Fujitsu specialist support staff to perform the request and link to the Bonded TfSNow Incident.
 - b. The Fujitsu MAC team will then assign the bonded Incident to the relevant Fujitsu team, this will raise a Peak reference allowing updates to be visible to POL.
4. If Fujitsu approval has not been granted:



- a. Fujitsu MAC team will update the bonded TfSNow Incident and notify POL that the process will need to restart as Fujitsu approval has not been granted.

5.3.4 Grant Additional Elevated Privileges - if required

If additional temporary elevated privileges have been cited as needed, then a process is followed to grant the relevant Fujitsu specialist support staff with the privileges required.

1. The relevant team will pass the Peak (raised from the bonded Incident) to the CSPOA Security team for additional temporary elevated privileges to be granted. The Peak will confirm Date and Time access is required.
2. CSPOA Security check the TfSNow Incident for agreed POL and Fujitsu approvals and that the request is being made within the stated timeframe. If the required approvals are not supplied, or the timeframe is incorrect, then the request will be denied, and new timeframes will need to be agreed.
3. If the approvals have been supplied and the timeframe is correct, then CSPOA Security will raise an internal TfSNow Incident requesting additional temporary elevated privileges and pass to the UNIX team.
4. CSPOA Security will update the Peak with the internal TfSNow Incident reference and pass the Peak back to SSC
5. The UNIX team will grant access to the stated Fujitsu support specialist at the start time required and will contact the required Fujitsu specialist support staff and confirm additional temporary elevated privileges have been granted. The UNIX team will update the Incident confirming access has been granted clearly showing the command has been run with result (see figure below for example of the type of evidence required). If for any reason TfSNow is not available, then the UNIX team will need to confirm the time of the command being run to CSPOA Security and a TfSNow update will be required when TfSNow is operational again.

SQL> grant appsup to ops\$(MSAD)

Grant succeeded.

Figure 1: Example of Grant succeeded

6. CSPOA Security will update the Peak with the Date/Time when access was granted by UNIX
7. Once the required actions have been completed, the Fujitsu specialist support staff member who was granted additional temporary elevated privileges will contact the UNIX team for access to be revoked.
8. The Unix team will revoke the additional temporary elevated privileges and update the TfSNow internal Incident immediately confirming access has been revoked and clearly showing the command has been run with result before passing the Incident back to the CSPOA Security team (see figure below for example of the type of evidence required). If for any reason TfSNow is not available, then the UNIX team will need to confirm the time of the command being run to CSPOA Security and a TfSNow update will be required when TfSNow is operational again.

SQL> revoke appsup from ops\$(MSAD);

Revoke succeeded.

Figure 2: Example of Revoke succeeded

9. CSPOA Security will also monitor the timeframe and if they do not receive a confirmation from the Unix team by the stated deadline then CSPOA Security will initiate the revocation process.
10. CSPOA Security will update Peak with the date/time the access was revoked.
11. CSPOA Security will close the TfSNow internal Incident.



5.3.4.1 Reporting on Granting of Additional Temporary Elevated Privileges

The granting of additional temporary elevated privileges is recorded using the Fujitsu and POL service management toolsets and can be reviewed by either party using its own system.

In addition, Fujitsu also report on the granting of additional elevated privileges within the monthly Fujitsu SecOps report which is shared with POL for its Information Security Management Forum (ISMF) meeting.

5.3.5 Make the data change

Once the Fujitsu specialist support staff are ready to make the required change, the following process is followed:

1. The Fujitsu specialist support staff perform the actions detailed on the Change, whilst capturing evidence of the pre and post implementation states, alongside the committed actions. The actions will be recorded in the Peak.
2. Within the SSC, one member of the SSC will perform the data correction while a second member of the SSC will witness the change being made. The witness will be recorded in the Peak.
3. The Fujitsu MAC team add the evidence to the Change and the to the TfSNow bonded Incident. See examples in Appendix B – Evidence Examples.

5.3.6 End the process – closing the Incident

Once the required data changes have been made the process of closing the Incident and the Horizon Data Change Process is performed.

1. The Fujitsu specialist support staff close the Peak with comments and action completed.
2. The Fujitsu specialist support staff close the Change checking evidence has been attached.
3. The bonded Incident with evidence is passed back to POL to review and confirm Incident closure.
4. POL to confirm the Incident can be closed.
5. POL and Fujitsu close the Incident.

5.4 Reporting on Horizon Data Changes

The actions are recorded within the bonded Incident using the Fujitsu and POL service management toolsets and can be reviewed by either party at any time using its own system.

6 Continuous Improvement

If, whilst performing any of these actions, Fujitsu identifies a potential defect in any system or process that requires investigation and a potential fix – whether that would reduce the likelihood of the need to perform these actions in the future or not – then Fujitsu will raise a Defect which will then be handled under the POA Live Defect Management process.



Appendix A – POL Ad-hoc Form Example

The following is a current example of the POL Ad-hoc form supplied by POL at the date of this

Date of request:	
Name of person raising the request:	
Type of Request:	
Reason for Request:	
Confirm the actions to be taken:	
What is the technical risk / impact?	
What is the business risk / impact?	
Files which require removal:	
Additional information:	

document.



HORIZON DATA CHANGES PROCESS WORK INSTRUCTION

FUJITSU RESTRICTED (COMMERCIAL IN CONFIDENCE)



Appendix B – Evidence Examples

B.1 SQL Evidence

PRE EVIDENCE (SQL looking for branch user/stock unit)

```
select u.branch_user, u.stock_unit, to_char(l.last_logon_timestamp, 'DD-Mon-YYYY HH24:MI:SS') last_logon
from ops$brdb.brdb_branch_users u
left join ops$brdb.brdb_branch_user_last_logon l
on u.branch_accounting_code = l.branch_accounting_code
and u.fad_hash = l.fad_hash
and u.branch_user = l.branch_user
where u.branch_accounting_code = 109008
and u.fad_hash = 80
and u.stock_unit = 'PX';
```

OUTPUT FROM SQL ABOVE

BRANCH_USER STO LAST_LOGON

\$\$PX50 PX 18-Dec-2019 15:15:19

STATEMENT – (update PX to DEF, Conformation appears below that 1 record has been updated)

```
update ops$brdb.brdb_branch_users
set stock_unit = 'DEF'
where branch_accounting_code = 109008
and fad_hash = 80
and branch_user = '$$PX50'
```

1 row updated.

POST EVIDENCE (Displays the branch user/stock unit)

```
SQL> select branch_user, stock_unit
from ops$brdb.brdb_branch_users
where branch_accounting_code = 109008
and fad_hash = 80
and branch_user = '$$PX50'; 2 3 4 5
```

BRANCH_USER STO (Output from SQL)

\$\$PX50 DEF

SQL> commit; (Writing to database, conformation from database below)

Commit complete.

B.2 File Removal Evidence

PRE EVIDENCE

```
[IRRELEVANT] ls -lrt /app/brdb/trans/externalinterface/input_share (List files in directory)
-rw-rw---- 1 podguser pathway 8478920 Apr 8 03:33 CA202104061000003920.TAN
[IRRELEVANT]
```

COMPLETING ACTION

```
[IRRELEVANT] rm CA202104061000003920.TAN (Remove file)
```

POST EVIDENCE

```
[IRRELEVANT] brdb:>pwd (Displays the present working directory as detailed below)
/app/brdb/trans/externalinterface/input_share
```

```
[IRRELEVANT] brdb:>ls -l *TAN (This will list any files in the directory that match *TAN, Line below shows there are no files matching)
ls: cannot access *TAN: No such file or directory
```