FUJ00162527

From: Jonathan Gribben[jonathan.gribben@GRO]

Sent: Tue 19/02/2019 6:35:26 PM (UTC)

To: Lenton, Matthew[Matthew.Lenton@GRO]

Cc: Andrew Parsons[andrew.parsons@GRO]; Lucy Bremner[lucy.bremner@GRO]; Emma Campbell-Danesh[emma.campbell-danesh@GRO]; Ibbett, Dave[Dave.Ibbett@GRO]; Parker, Steve[ParkerSP@GRO]; Godeseth, Torstein[Torstein.O.Godeseth@GRO]; Newsome, Pete[pete.newsome@GRO]; Jay, Christopher[Christopher.Jay@GRO]; Defence Legal (Chris Jay,)[Legal.Defence@GRO]; Michael Wharton[michael.wharton@GRO]

Subject: Remote access - urgent [WBDUK-AC.FID27032497]

Attachment: _DOC_154352282(1)_Remote Access - JG 19_2_19.DOCX

Matthew,

Michael has reviewed the four documents that you referred to in your email and produced lists of what appear to be the different levels of remote access and the various roles/user types which may have a degree of remote access – see below. The lists are significantly longer than we were anticipating and they appear to contradict Torstein's evidence on remote access (which talks about privileged users and SSC injecting transaction data only). I'm sure there is an explanation for this, but we will need help from Fujitsu to square the circle.

When we spoke on Monday I explained that we needed to produce a table which summarises the different types of remote access and the key information relating to each type. I attach a very first draft of the table. This may give the task some focus.

This is a top priority – to discuss on tomorrow morning's call please.

Kind regards

Jonny

RS/REQ/023

- PWYDCS\SSC Apps SUP
- PWYDCS\SSC Apps MAN
- PWYDCS\Operational MAN
- PWYDCS\Application SUP
- SSC Apps MAN
- SSC Apps SUP
- Operational MAN
- Application SUP
- SYSMAN\SMC
- SYSMAN\MSS
- NT Administrator User
- TSadmin Role
- SSHadmin Role
- PWYDCS Users
- HUTHTIP Users
- PDRTIP Users
- PWYKMS Users
- PWYCSM Users
- SYSMAN Users
- Secure Access Server Users
- Counter Access Users
- NT Data Centre System Access Users
- SSC Support Group
- SMC Support Group
- MSS Support Group

FUJ00162527

- Operational Management Support Group

RS/DES/047

- KMS Security Manager
- KMS Database administrator
- KMS Key Manager
- KMA Data Manager
- PO Key Recovery at Systems Management Centre (SMC)
- KMS Application support at System Support Centre (SSC)
- KMS Systems Administrators
- Computer operator
- Maestro administrator
- Audit of Key Management System
- KMS auditor
- Engineer
- SW_Internal
- SW_External
- KMSsql
- Maestro
- DBA Batch
- Tivoli_Status_Check
- Tivoli
- CAW Security Manager
- CAW Key Manager
- CAW VPN Key Manager
- CAW Maintenance User
- CAW Auditor

DES/SEC/HLD/1045

- IS-Unix/IS-NT
- IS-DBA
- MSS/SMG
- SSC
- SAP Basis
- Network Managers
- Emergency root access

SVM/SEC/PRO/1780

- SSN access
- Operating system access – Unix
- Software access – SSN
- Database access – remote
  - Transaction Enquiry Service database access
  - Data Reconciliation Service database access
  - APOP database access
- Database access
  - SQL Server database access
  - Oracle database access

Jonathan Gribben
Managing Associate
Womble Bond Dickinson (UK) LLP

d: GRO

FUJ00162527

m: GRO
t:
e:
Stay informed: sign up to our e-alerts

WOMBLE BOND DICKINSON

womblebonddickinson.com

From: Matthew.Lenton@ GRO [mailto:Matthew.Lenton@ GRO]
Sent: 14 February 2019 10:43
To: Jonathan Gribben
Cc: Andrew Parsons; Lucy Bremner; Emma Campbell-Danesh; Dave.Ibbett@ GRO ; ParkerSP@ GRO ; Torstein.O.Godeseth@ GRO ; pete.newsome@ GRO ; Christopher.Jay@ GRO ; Legal.Defence@ GRO
Subject: RE: Injecting transactions - urgent

Jonny,

Our responses to your questions below, in bold.

The Claimants have added several documents to the Horizon Issues Trial that relate to "remote access", so we need to be very clear about the different levels of access and how that has changed since Horizon was introduced.
There has always been segregation of duties. Those with infrastructure access did not have the business knowledge to inject transaction data.

1. Have the Belfast team (i.e. true "Privileged Users") had permanent enhanced access to allow them to fully support the service and estate since Horizon was introduced in 1999?
    a. ***LEGACY: There was no permanent enhanced access: users would need to switch on enhanced capability, which would generate an audited event, i.e. you'd need to change role.***
    b. ***HNG-X: Ditto.***
    c. ***Present: Ditto.***
2. Please provide a list of the other levels of access referred to by Jason (examples given are the Security team for Cryptographic Material management, SSC to access the counter logs, DBA's etc) and explain: (1) exactly what access they have; and (2) whether the position has been the same since Horizon was introduced (if not, please explain the changes).
    a. ***LEGACY:***
        i. ***RS/REQ/023 SECURE SUPPORT ROLE DEFINITIONS FOR SECURENT TERMINAL SERVER BUILDS***
        ii. ***RS/DES/047 KMS ROLES, ACCESS CONTROLS AND NT DOMAIN STRUCTURE***
    b. ***HNG-X:***
        i. ***DES/SEC/HLD/1045 HNGX SUDO SUPPORT REQUIREMENTS***
        ii. ***SVM/SEC/PRO/1780 SERVICE DELIVERY UNITS ROLES RESPONSIBILITIES AND ACCESS REQUIREMENTS***
    c. ***Present: As HNG-X***
3. Who/what are DBAs?
    a. ***Database Administrator – defined as per industry norms. The role provides the segregation of duties between those who set up and manage the database, and those who manage the daily operations.***
4. Who can add, edit, delete data in database administration?
    a. ***LEGACY, HNG-X and Present: Members of the Belfast DBA and Unix teams, but would require enhanced access, as in 1 above.***
5. Who can add, edit, delete data in the key management server?
    a. ***LEGACY: RS/DES/047 KMS ROLES, ACCESS CONTROLS AND NT DOMAIN STRUCTURE***
    b. ***HNG-X: Members of the Belfast DBA and Unix teams, but would require enhanced access, as in 1 above. Sec Ops for day to day activities using the KSN workstation located in a secure room.***
    c. ***Present: as for HNG-X.***
6. We also need to be clear about how such access was audited.

FUJ00162527

a. ***LEGACY: Event management system scrapes the system logs looking for events identified as security or audit (SYSMAN documentation). This is then recorded in a separate system which is not accessible to the privileged users noted above.***
b. ***HNG-X: Ditto***
c. ***Present: Ditto***

Matthew Lenton
Post Office Account Document Manager
P&PS, Digital Technology Services

Fujitsu
Lovelace Road, Bracknell, Berkshire, RG12 8SN
Phone: GRO
Email: matthew.lenton@ GRO
Web: https://www.fujitsu.com/global/

From: Jonathan Gribben [mailto:jonathan.gribben@ GRO]
Sent: 14 February 2019 07:58
To: Lenton, Matthew <Matthew.Lenton@ GRO >; Muir, Jason <Jason.Muir@ GRO >; Ibbett, Dave <Dave.Ibbett@ GRO >; Parker, Steve <ParkerSP@ GRO >; Gareth Jenkins <gi.jenkins@ GRO >; Newsome, Pete <pete.newsome@ GRO >; Jay, Christopher <Christopher.Jay@ GRO >; Defence Legal (Chris Jay,) <Legal.Defence@ GRO >
Cc: Andrew Parsons <andrew.parsons@ GRO >; Lucy Bremner <lucy.bremner@ GRO >; Emma Campbell-Danesh <emma.campbell-danesh@ GRO >
Subject: RE: Injecting transactions - urgent

Matthew,

We want to create a document which sets out the different levels of "remote access", who had that access and how it was audited, starting from 1999 to the present day. That document should also refer to the controls that have been in place regarding the use of remote access across the whole period.

We appreciate that there have been lots of changes since Horizon was introduced and that it will take time to gather the information needed to produce a document spanning the entire period. Therefore, as an interim measure, I suggested that we aim to produce a document which sets out the above information at certain points in time, namely:-

1. when Horizon was introduced;
2. when Horizon Online was introduced;
3. the present day.

At this stage it would also be helpful for Fujitsu to call out any significant changes that have been introduced in between those points in time. For example, on yesterday's call you mentioned the introduction of the SSH logging server in 2004.

Please let me know if you'd like to discuss this further. Otherwise, please let me know when we can expect to receive a response.

Kind regards
Jonny

Jonathan Gribben
Managing Associate
Womble Bond Dickinson (UK) LLP

d:
m:
t:
e: GRO

FUJ00162527

Stay informed: sign up to our e-alerts

womblebonddickinson.com

From: Matthew.Lenton@GRO [mailto:Matthew.Lenton@GRO]
Sent: 13 February 2019 17:37
To: Jonathan Gribben; Jason.Muir@GRO; Dave.Ibbett@GRO; ParkerSP@GRO; Gareth Jenkins; pete.newsome@GRO; Christopher.Jay@GRO; Legal.Defence@GRO
Cc: Andrew Parsons; Lucy Bremner; Emma Campbell-Danesh
Subject: RE: Injecting transactions - urgent [WBDUK-AC.FID123822914]

Jonny,

On the call earlier you suggested the approach that you'd like us to take in responding to the questions below. Would you mind repeating that here – as you may have gathered I was disconnected from the call and unable to get back in.

We will be looking at this question first thing in the morning so your suggestion would be welcome before then please.

Matthew Lenton
Post Office Account Document Manager
P&PS, Digital Technology Services

Fujitsu
Lovelace Road, Bracknell, Berkshire, RG12 8SN
Phone: GRO
Email: matthew.lenton@GRO
Web: https://www.fujitsu.com/global/

From: Jonathan Gribben [mailto:jonathan.gribben@GRO]
Sent: 13 February 2019 10:06
To: Muir, Jason <Jason.Muir@GRO>; Ibbett, Dave <Dave.Ibbett@GRO>; Parker, Steve <ParkerSP@GRO>; Gareth Jenkins <gi.jenkins@GRO>; Newsome, Pete <pete.newsome@GRO>; Jay, Christopher <Christopher.Jay@GRO>; Defence Legal (Chris Jay,) <Legal.Defence@GRO>
Cc: Andrew Parsons <andrew.parsons@GRO>; Lucy Bremner <lucy.bremner@GRO>; Emma Campbell-Danesh <emma.campbell-danesh@GRO>; Lenton, Matthew <Matthew.Lenton@GRO>
Subject: RE: Injecting transactions - urgent [WBDUK-AC.FID123822914]

Dear all,
Thank you for the additional comments.

The Claimants have added several documents to the Horizon Issues Trial that relate to "remote access", so we need to be very clear about the different levels of access and how that has changed since Horizon was introduced.

1. Have the Belfast team (i.e. true "Privileged Users") had permanent enhanced access to allow them to fully support the service and estate since Horizon was introduced in 1999?
2. Please provide a list of the other levels of access referred to by Jason (examples given are the Security team for Cryptographic Material management, SSC to access the counter logs, DBA's etc) and explain: (1) exactly what access they have; and (2) whether the position has been the same since Horizon was introduced (if not, please explain the changes).
3. Who/what are DBAs?
4. Who can add, edit, delete data in database administration?
5. Who can add, edit, delete data in the key management server?

FUJ00162527

We also need to be clear about how such access was audited. We have some information on this already and once the above questions have been answered I'll work out if there are any gaps.
Please would you respond ASAP today.
Kind regards
Jonny

Jonathan Gribben
Managing Associate
Womble Bond Dickinson (UK) LLP

d:
m:
t:
e: GRO

Stay informed: sign up to our e-alerts

WOMBLE BOND DICKINSON

womblebonddickinson.com

From: Jason.Muir@ GRO [mailto:Jason.Muir@ GRO]
Sent: 12 February 2019 16:27
To: Dave.Ibbett@ GRO ; ParkerSP@ GRO ; Jonathan Gribben; Gareth Jenkins; pete.newsome@ GRO ; Christopher.Jay@ GRO ; Legal.Defence@ GRO
Cc: Andrew Parsons; Lucy Bremner; Emma Campbell-Danesh; Matthew.Lenton@ GRO
Subject: RE: Injecting transactions - urgent [WBDUK-AC.FID123822914]

All,

I have added my comments below inline.

Regards,

Jason Muir

Operational Security Manager

Post Office Account

Fujitsu

Mob: GRO

From: Ibbett, Dave
Sent: 12 February 2019 15:16
To: Parker, Steve <ParkerSP@ GRO ; Jonathan Gribben <jonathan.gribben@ GRO >; Gareth Jenkins <gi.jenkins@ GRO >; Newsome, Pete <pete.newsome@ GRO >; Jay, Christopher <Christopher.Jay@ GRO >; Defence Legal (Chris Jay,) <Legal.Defence@ GRO >; Muir, Jason <Jason.Muir@ GRO >
Cc: Andrew Parsons <andrew.parsons@ GRO >; Lucy Bremner <lucy.bremner@ GRO >; Emma Campbell-Danesh <emma.campbell-danesh@ GRO >; Lenton, Matthew <Matthew.Lenton@ GRO >

FUJ00162527

Subject: RE: Injecting transactions - urgent [WBDUK-AC.FID123822914]

Adding in Jason for the SECOPS section and copying Matthew for recording.

Regards,

Dave

From: Parker, Steve
Sent: 12 February 2019 15:00
To: Jonathan Gribben <jonathan.gribben@GRO>; Gareth Jenkins <gi.jenkins@GRO>; Ibbett, Dave <Dave.Ibbett@GRO>; Newsome, Pete <pete.newsome@GRO>; Jay, Christopher <Christopher.Jay@GRO>; Defence Legal (Chris Jay,) <Legal.Defence@GRO>
Cc: Andrew Parsons <andrew.parsons@GRO>; Lucy Bremner <lucy.bremner@GRO>; Emma Campbell-Danesh <emma.campbell-danesh@GRO>
Subject: RE: Injecting transactions - urgent [WBDUK-AC.FID123822914]

Jonny,

Comments from me below in red. This is the first time I've seen the comments from Deloitte.

Steve

From: Jonathan Gribben <jonathan.gribben@GRO>
Sent: Tuesday, February 12, 2019 2:13 PM
To: Gareth Jenkins <gi.jenkins@GRO>; Ibbett, Dave <Dave.Ibbett@GRO>; Newsome, Pete <pete.newsome@GRO>; Jay, Christopher <Christopher.Jay@GRO>; Defence Legal (Chris Jay,) <Legal.Defence@GRO>
Cc: Andrew Parsons <andrew.parsons@GRO>; Lucy Bremner <lucy.bremner@GRO>; Parker, Steve <ParkerSP@GRO>; Emma Campbell-Danesh <emma.campbell-danesh@GRO>
Subject: RE: Injecting transactions - urgent [WBDUK-AC.FID123822914]
Importance: High

Dear all,

Further to and in addition to my question for Gareth below, please would you let me know, as soon as possible, whether the Belfast team and Privileged Users are one and the same thing, or are there more Privileged Users? Has the position been the same since Horizon was introduced in 1999/2000? If it has changed, please describe the changes. I've attached an email which contains some comments from Gareth that these questions are seeking to clarify.
The Belfast operations team have privileged access to Horizon and hence are Privileged users. In the context of being able to inject transactions they would have the access but not the knowledge to generate the business transactions. There are a number of different privileged roles which SecOps can describe. **(JM: As a general rule when we talk about "Privileged Users" we are talking about the Belfast team as they have permanent enhanced access to allow them to fully support the service and estate. There are however many different levels of access which are based on the users role which may or may not be regarded as privilege access, some examples may be the Security team for Cryptographic Material management, SSC to access the counter logs, DBA's etc. The level of access given is appropriate to the role the user is performing. Ie principle of minimal privilege where by a user is given the minimum amount of privileges to enable them to do their job without having access over and above what is required)**

Also, how does the statement that "all transactions are digitally signed in HNG-X so spoofing can't happen" reconcile with the finding by Deloitte that:-

FUJ00162527

> "There are a limited number of Privileged Users (25 at the time of testing – June 2016) who could theoretically (due to the segregation of duties breach between database administration and the key management server) amend the Message Log for one or more Counters in one or more branches and make the transaction/s amended, look legitimate when it is retrieved from the Audit Store (through spoofing of the digital signature)".

This appears to be describing people with privileged access which would allow them to amend audit trails. SSC do not have this access (by design). I'm not sure who has such access, SecOps would need to confirm. Deloitte's comment imply that the level of access applied to security and database admin staff. Assuming that is the case, these people would be described as having access to audit trail but not having the level of Horizon knowledge to craft the fraudulent business transactions to inject. **(JM: Im not aware that anyone has access to be able to amend audit trails, roles between key management and database admin are strictly segregated. Access to key material has multiple controls in place to prevent unauthorised access and so it is highly unlikely that a breach between database admin and key management has taken place. Even if it were its unlikely each of the opposing capability would have enough knowledge to effectively initiate such an amendment to the audit trail.)**

Also, are the Privileged Users referred to by Deloitte separate from those in SSC who can inject Balancing Transactions?
As above, my reading is that Deloitte are describing people with access to audit trail, so yes, separated from SSC. Without a definition of the roles Deloitte were describing in their report, I cannot be sure.

Please would you get back to me ASAP today.
Kind regards
Jonny

Jonathan Gribben
Managing Associate
Womble Bond Dickinson (UK) LLP

d: GRO
m:
t:
e:

Stay informed: sign up to our e-alerts

WOMBLE BOND DICKINSON

womblebonddickinson.com

From: Jonathan Gribben
Sent: 12 February 2019 12:34
To: 'Gareth Jenkins'; Dave.Ihbett@GRO; pete.newsome@GRO; Christopher.Jay@GRO; Legal.Defence@GRO
Cc: Andrew Parsons; Lucy Bremner; ParkerSP@GRO; Emma Campbell-Danesh
Subject: RE: Injecting transactions - urgent [WBDUK-AC.FID27032497]

Hi Gareth,

Thank you for this.

I can't see any specific comments from Friday in the attachment – do you mean Thursday when you added the red [GIJ] comments?
Kind regards

FUJ00162527

Jonny

From: Gareth Jenkins [mailto:gi.jenkins@GRO]
Sent: 11 February 2019 10:11
To: Dave.Ibbett@GRO; Jonathan Gribben; pete.newsome@GRO; Christopher.Jay@GRO; Legal.Defence@GRO
Cc: Andrew Parsons; Lucy Bremner; ParkerSP@GRO; Emma Campbell-Danesh
Subject: RE: Injecting transactions - urgent [WBDUK-AC.FID27032497]

Hi Jonny,

Dave's email doesn't include my specific responses that I prepared on Friday.

These are in the attached email. Note that the comments I made on Saturday were meant as clarification to my note on Friday.

Hopefully it all makes sense.

Best wishes

Gareth

From: Dave.Ibbett@GRO [mailto:Dave.Ibbett@GRO]
Sent: 11 February 2019 09:57
To: Jonathan Gribben <jonathan.gribben@GRO>; Gareth Jenkins <gi.jenkins@GRO>; pete.newsome@GRO; Christopher.Jay@GRO; Legal.Defence@GRO
Cc: Andrew Parsons <andrew.parsons@GRO>; Lucy Bremner <lucy.bremner@GRO>; ParkerSP@GRO; Emma Campbell-Danesh <emma.campbell-danesh@GRO>
Subject: RE: Injecting transactions - urgent [WBDUK-AC.FID27032497]

Hi Jonny,

Please see below from Gareth over the weekend. Matthew supplied Gareth some documentation to go through resulting in the detail below.

I've had a quick scan and they confirm the following:

1. All AP Transactions in Old Horizon were digitally signed at the counter and so cannot be spoofed by SSC
2. All Banking Transactions are digitally signed at the counter and so cannot be spoofed by SSC
3. (NB all transactions are digitally signed in HNG-X so spoofing can't happen).

That means that the only transactions that could possibly be injected by SSC to benefit them (as opposed to re-injecting copies of missing transactions that have been recovered) are EPOSS Transactions, which mean Giro Deposits and Manual Banking Deposits.

Regards,

Dave

From: Jonathan Gribben [mailto:jonathan.gribben@GRO]
Sent: 10 February 2019 22:39

FUJ00162527

To: Gareth Jenkins <gi.jenkins@ GRO >; Newsome, Pete <pete.newsome@ GRO >; Jay, Christopher <Christopher.Jay@ GRO >; Defence Legal (Chris Jay,) <Legal.Defence@ GRO >
Cc: Andrew Parsons <andrew.parsons@ GRO >; Ibbett, Dave <Dave.Ibbett@ GRO >; Lucy Bremner <lucy.bremner@ GRO >; Parker, Steve <ParkerSP@ GRO >; Emma Campbell-Danesh <emma.campbell-danesh@ GRO >
Subject: RE: Injecting transactions - urgent [WBDUK-AC.FID27032497]

Evening all,

Please would you let me know when we can expect to receive FJ's response to my email below. We need to issue the letter to Freeths ASAP this week as we are in Court for a pre trial review on Thursday.

Many thanks
Jonny

Jonathan Gribben
Managing Associate
Womble Bond Dickinson (UK) LLP

d:
m: GRO
t:
e:

Stay informed: sign up to our e-alerts

WOMBLE BOND DICKINSON

womblebonddickinson.com

From: Gareth Jenkins [mailto:gi.jenkins@ GRO]
Sent: 07 February 2019 16:26
To: Jonathan Gribben; pete.newsome@ GRO ; Christopher.Jay@ GRO ; Legal.Defence@ GRO
Cc: Andrew Parsons; Dave.Ibbett@ GRO ; Lucy Bremner; ParkerSP@ GRO ; Emma Campbell-Danesh
Subject: RE: Injecting transactions - urgent [WBDUK-AC.FID27032497]

Hi,

I've received mine and commented to others in Fujitsu. I assume that someone will forward a consolidated set of comments to you.

Best wishes

Gareth

From: Jonathan Gribben [mailto:jonathan.gribben@ GRO]
Sent: 07 February 2019 14:03
To: Gareth Jenkins <gi.jenkins@ GRO >; pete.newsome@ GRO ; Christopher.Jay@ GRO ; Legal.Defence@ GRO
Cc: Andrew Parsons <andrew.parsons@ GRO >; Dave.Ibbett@ GRO ; Lucy Bremner

FUJ00162527

<lucy.bremner@GRO>; ParkerSP@GRO Emma Campbell-Danesh <emma.campbell-danesh@GRO
GRO>
Subject: RE: Injecting transactions - urgent [WBDUK-AC.FID27032497]

Gareth, Pete, Chris and Dave,

Please confirm whether or not you received my email below. I re-sent it with the attachments split across two emails as the first one bounced back.

Kind regards

Jonny

Jonathan Gribben
Managing Associate
Womble Bond Dickinson (UK) LLP

d:
m:
t:
e: GRO

Stay informed: sign up to our e-alerts

WOMBLE BOND DICKINSON

womblebonddickinson.com

From: Jonathan Gribben
Sent: 06 February 2019 20:01
To: 'Gareth Jenkins'; 'pete.newsome@GRO'; 'Christopher.Jay@GRO'; 'Legal.Defence@GRO'
Cc: Andrew Parsons; 'Dave.Ibbett@GRO'; Lucy Bremner; 'ParkerSP@GRO'; Emma Campbell-Danesh (emma.campbell-danesh@GRO)
Subject: Injecting transactions - urgent [WBDUK-AC.FID27032497]

Dear all,

Privileged & Confidential – please do not forward

Apologies in advance for the length of this email.

Exec Summary

Paragraph 35 of Steve's second statement is not entirely correct. We have been looking into this subject further and below is a summary of our investigation.

We need to send Freeths a letter to clarify the correct position. I have summarised the key points and set out some questions below along with a summary of our investigation. Please would you review those let me know the responses/whether anything is incorrect by midday tomorrow. Once this has been done we will draft a letter to Freeths correcting the position that we will ask you to review and confirm before it is issued.

Summary of key points/questions

FUJ00162527

Key points:-

- Post Office offered personal banking (manual) for a number of institutions from the introduction of Horizon;
- it would have been possible for a rogue SSC employee to inject a cash deposit into their personal banking account;
- a customer's account would not be credited until the paper deposit slip reached the relevant financial institution (need to confirm this for Girobank), so the rogue SSC employee would not benefit from injecting a transaction because there would be no corresponding paper deposit slip (query whether a TC would be issued due to the absence of the paper deposit slip);
- online banking transactions were introduced in 2003 and Gareth does not know if it would even be possible to get around the encryption issues that would be present if someone tried to insert an "automated" transaction; and
- there are some other transactions that the rogue SSC employee could have injected – for manual transactions there may be a paper trail (TBC on a transaction by transaction basis) and for online (i.e. automated) transactions the position would be the same as per online banking transactions (i.e. encryption issues).

Questions:-

- were online Girobank transactions AP transactions?
- does AP mean automated?;
- what would a rogue SSC employee have to do to in order to inject an online/automated transaction (i.e. please articulate the encryption issues and describe what would have to be done to theoretically get around them, including references to any controls designed to prevent this)?

Summary of investigation into injecting transactions in Legacy Horizon

Paragraph 35 of Steve's statement reads:-

> "*With reference to Dr. Worden's statement that "as for transferring money, Horizon includes no functionality that allows payments to be made to external parties or account", at paragraphs 20.1, 20.3, 21 and 58.4 of my first statement I said that money could not be transferred, by which I mean that it could not be transferred into a third party's bank account. I have given this matter further thought and discussed it with my colleagues and we have now theorised that someone could have carried out a Post Office transaction, such as a GIRO bank transfer2 or a utility bill payment. A GIRO bank transfer inserted by someone at SSC would have been detected as part of Post Office's reconciliation processes because there would be no accompanying paper document. There is no accompanying paper document for a utility bill payment, so in theory such a transaction would not be detected through reconciliation. I am not aware of any such activity ever taking place and if it had occurred it would have resulted in instant dismissal.*
>
> *2 A Giro bank is also an AP transaction (like bill payments). It is the only type of bank account that is. All other banking deposits go through a totally different path*."

After the statement had been submitted, Gareth provided the following comments:-

1. The Giro Bank Transactions are not AP, but standard EPOSS Transactions. I don't know how info on them got to Giro Bank – it may well be that Giro Bank worked off the paper trail and then sent summaries to POL which they then reconciled with the Horizon feed. POL would need to provide the details.

2. Prior to online banking (introduced in 2003), POL did support some (but not all) other banks with deposit and cheque cashing facilities. Again these were EPOSS (not AP) transactions. I assume that there was also a paper trail here and it would work in a similar way to Giro Bank. Again it is POL that need to define the process. All Horizon did was provide the buttons to record the electronic part of the transaction.

Please find attached the following documents:

1. Post Office's Counter Operations Manual for Personal Banking (version 1 August 2001) which sets out the procedure for accepting cash deposits other than Alliance & Leicester Giro services (see the comment on

FUJ00162527

page 2 re Alliance & Leicester Giro services being distinct and separate from those that appear in this booklet and can be found in the Alliance & Leicester Giro booklet – Post Office have not yet been able to locate the corresponding version of this booklet but has provided version 3 from March 2007 – see point 3 below) and states that cash is not deposited into a customer's account until the paper deposit document reaches their bank (section 5.9 on page 9).

2. Post Office's Operational Focus 0203 from 3 – 9 April 2003 which contains a list of banking services available at branches from Tuesday 1 April 2003 and shows that Post Office accepted cash deposits from seven banks. All of them are stated to be "manual", apart from Alliance & Leicester/Giro Bank which is stated to be "automated or manual". Manual means paper based and automated means online using a card.

3. Post Office's Operations Manual for Alliance & Leicester Personal Banking (version 3 March 2007). This version shows that Post Office did not offer manual Alliance & Leicester personal banking by March 2007 – it was online banking only.

4. Post Office's Horizon System User Guide / Balancing with Horizon Guide (version 1 28 July 2000). This Balancing with Horizon Guide Section 1 deals with Personal Banking (page 734 of the PDF) and Alliance & Leicester Girobank (page 743 of the PDF). It was a requirement to rem out paper deposit slips on a daily basis. There was also an opportunity for branches to reconcile the Horizon record of deposit transactions with the paper deposit slips they were holding as part of this process.

The distinction between online and manual banking transactions is that it would have been possible for SSC to insert a "manual" transaction, but Gareth does not know if it would even be possible to get around the encryption issues that would be present if someone tried to insert an "automated" transaction. Automated deposit transactions required the customer's card to be swiped through the PIN Pad, which would add in some crypto data that prevents SSC being able to mimic this step.

In terms of other transactions that could have potentially been injected for personal benefit, based on the list of products and services available in branches as at July 2005 as per the attached welcome pack Gareth has advised that:-.

- it may have been possible to inject bill payment transactions to pay a bill (i.e. the utility bill example given in Parker 2, for which there would be no paper trail/reconciliation);
- telephony transactions were all online, so the position is the same as online banking transactions (i.e. encryption issues);
- banking/savings – covered above;
- national savings and investments – a mix of online and offline. We are checking with Post Office whether there was a paper trail for the offline ones;
- money transfer – online; and
- the rest did not involve any accounts to credit and therefore the rogue SSC employee wouldn't benefit.

FUJ00162527

Unless otherwise stated, this email has been sent from Fujitsu Services Limited (registered in England No 96056); Fujitsu EMEA PLC (registered in England No 2216100) both with registered offices at: 22 Baker Street, London W1U 3BW; PFU (EMEA) Limited, (registered in England No 1578652) and Fujitsu Laboratories of Europe Limited (registered in England No. 4153469) both with registered offices at: Hayes Park Central, Hayes End Road, Hayes, Middlesex, UB4 8FE.
This email is only for the use of its intended recipient. Its contents are subject to a duty of confidence and may be privileged. Fujitsu does not guarantee that this email has not been intercepted and amended or that it is virus-free.
Unless otherwise stated, this email has been sent from Fujitsu Services Limited (registered in England No 96056); Fujitsu EMEA PLC (registered in England No 2216100) both with registered offices at: 22 Baker Street, London W1U 3BW; PFU (EMEA) Limited, (registered in England No 1578652) and Fujitsu Laboratories of Europe Limited (registered in England No. 4153469) both with registered offices at: Hayes Park Central, Hayes End Road, Hayes, Middlesex, UB4 8FE.
This email is only for the use of its intended recipient. Its contents are subject to a duty of confidence and may be privileged. Fujitsu does not guarantee that this email has not been intercepted and amended or that it is virus-free.
Unless otherwise stated, this email has been sent from Fujitsu Services Limited (registered in England No 96056); Fujitsu EMEA PLC (registered in England No 2216100) both with registered offices at: 22 Baker Street, London W1U 3BW; PFU (EMEA) Limited, (registered in England No 1578652) and Fujitsu Laboratories of Europe Limited (registered in England No. 4153469) both with registered offices at: Hayes Park Central, Hayes End Road, Hayes, Middlesex, UB4 8FE.
This email is only for the use of its intended recipient. Its contents are subject to a duty of confidence and may be privileged. Fujitsu does not guarantee that this email has not been intercepted and amended or that it is virus-free.