From:	Mark R Davies [_____ GRO _____]
Sent:	Fri 30/01/2015 1:40:30 PM (UTC)
To:	Melanie Corfield [_____ GRO _____]
Subject:	FW: Remote Access: in strictest confidence
Attachment:	image004.png
Attachment:	image003.png

Hi

Please can you have a look over this?

Best wishes,

Mark

Mark Davies I Communications and Corporate Affairs Director

1st Floor, Banner Wing, 148 Old Street, London, EC1V 9HQ

GRO 2 Postline [___ GRO ___]
2 Mobex [___ GRO ___]

[_____ GRO _____]

POST OFFICE

From: Lesley J Sewell
Sent: 30 January 2015 12:18
To: Mark R Davies
Subject: Fwd: Remote Access: in strictest confidence

Mark

Please see below.

L

Lesley J Sewell
Chief Information Officer
Post Office Ltd

Email [_____ GRO _____]
Direct: [
Mobile: **GRO**]

Sent from my iPad
Begin forwarded message:

> **From:** Julie George < [_____ GRO _____] >
> **Date:** 30 January 2015 12:09:57 GMT
> **To:** Lesley J Sewell < [_____ GRO _____] >
> **Subject: Fw: Fwd: Remote Access: in strictest confidence**

Here are the answers
Sent from Blackberry

From: Dave M King
Sent: Friday, January 30, 2015 12:04 PM
To: Julie George
Subject: RE: Fwd: Remote Access: in strictest confidence

There is no remote access to the terminals in branches. The only access channel is through the support network for software updates etc. There is nothing stored on the terminal all transactions are committed at the datacentre. It is not possible to instantiate a remote desktop session on a terminal and undertake transactions as if it were being done at that terminal

Dave King

Senior Technical Security Assurance Manager

2nd Floor,

I Future Walk,

Chesterfield, S49 1PF

GRO

From: Julie George
Sent: 30 January 2015 11:38
To: Dave M King
Subject: Re: Fwd: Remote Access: in strictest confidence

So can anyone remotely access sub postmasters horizon systems remotely and if they can I take it this would be visible and logged whether officially done or unofficially?
Sent from Blackberry

From: Dave M King
Sent: Friday, January 30, 2015 11:33 AM
To: Julie George
Subject: RE: Fwd: Remote Access: in strictest confidence

Julie

I have answered as best I can but I understand Kevin Lenihan is also getting the information from Fujitsu (I do know these have been answered for the lawyers and Deloitte when they were looking at this:

The system is pen tested for PCI yearly and at any major change (the last PCI test was between 03/06/2014 – 10/06/2014 and there was a test for the datacentre refresh which is not yet live in summer). There are not outstanding significant findings which have not been remediated.

Internal and external vulnerability scans are conducted monthly which have confirmed the lack of significant issues.

The system has remote access only for Fujitsu support personnel through a support gateway against which all activity is monitored.

All transactions are written to an immutable audit trail at the point of completion and it is from this store that any evidential information is obtained.

Thanks

Dave

Dave King
Senior Technical Security Assurance Manager

2nd Floor,
I Future Walk,
Chesterfield, S49 1PF

GRO

From: Julie George
Sent: 30 January 2015 11:13
To: Dave M King
Subject: Fw: Fwd: Remote Access: in strictest confidence

Dave can you address also words below marked in yellow and liaise with kevin lenehan he is sparrow liaison get back to me asap
Sent from Blackberry

From: Lesley J Sewell
Sent: Friday, January 30, 2015 09:58 AM
To: Dave Hulbert; Julie George
Subject: Fwd: Remote Access: in strictest confidence

Please see attached - current words being used

Lesley J Sewell
Chief Information Officer
Post Office Ltd

Email: l   **GRO**
Direct:
Mobile **GRO** 0

Sent from my iPhone
Begin forwarded message:

> **From:** Melanie Corfield   **GRO**
> **Date:** 30 January 2015 09:21:44 GMT
> **To:** Lesley J Sewell   **GRO**
> **Subject: Remote Access: in strictest confidence**

Hello Lesley
Below is the current Q and A we have been using on this, in liaison with Fujitsu (and which is in line with FOIs we have had on the subject).
Regarding the testing and standards, I have pasted below what we have said in FOI but this is from 2011 so might well have changed. Grateful for detail on this.
Many thanks
Mel

Remote Access
There are very concerning stories about remote access to Horizon that might have contributed or been the reason for unexplained changes being made to postmasters accounts - how do you explain changes to accounts at times when postmasters could not possibly have had access themselves?
- *Transaction data in branch accounts can't be changed remotely*
- *No evidence of malicious tampering*

There is very selective, misleading and incorrect information being put into the public
domain about a number of cases. Much of this is not actually included in any allegations or complaints put to us by applicants and also changes in nature and detail.
Post Office cannot breach the privacy and confidentiality of individual applicants by discussing their cases, even in the face of unsubstantiated, baseless or malicious allegations. To do so would lead to us being accused of breaching confidentiality and undermining the Scheme and mediation process. So we have been limited in the public comment we can make.
But there is no functionality in Horizon for either a branch, Post Office or Fujitsu to edit, manipulate or remove transaction data once it has been
recorded in a branch's accounts. It is possible for Fujitsu to view branch data in order to
provide support and conduct maintenance but this does not allow access to any functionality that could be used to edit recorded transaction data.
There is also no evidence at all of any malicious remote tampering.
So it is not possible to alter postmasters' accounts remotely?
It is not possible to edit or tamper with a transaction once it has been made.
It is possible to add transactions in order to make a correction. This is extremely rare, is carried out with the right level of security and it cannot be done without a postmaster's knowledge.
Can you rule out remote fraud or cybercrime?
There is no evidence at all of this in any of the investigations carried out - there is no evidence that Horizon has not worked as it should do. No company can completely prevent cybercrime but there is nothing to suggest that this has caused any of the issues that have been complained about.
We adhere to industry standards , regulatory and compliance requirements.
[Details to be provided separately]

From 2011 FOI. Post Office Ltd as a responsible business undertakes regular and robust external audits of its IT systems which includes Horizon. During the past five years there have 16 external audits and accreditations. Post Office Ltd undertakes monthly vulnerability scans and penetration tests are conducted annually, therefore there have been 65 scans and tests which we consider audits.

We also referred in another request to VocaLINK and the external consultancy IRM (Payment Card Industry audit). These audits cover the whole system including accounting, along with product and service end-to-end processes. In addition the following accreditations have been applied, British Standards Institute (BSI), security audit 270001 and VocalLink and Merchant Aquirer (Worldpay, Streamline HS

Mel Corfield
Communications Team
1st Floor - Old Street
Mobile: **GRO**