

To: 'Mark Underwood' [GRO] Harvey Michael [GRO] Kevin Lenihan [GRO]
Cc: Patrick Bourke [GRO]; Parsons, Andrew [GRO]
From: Newsome Pete [/o=Exchange/ou=AdminGroup1/cn=Recipients/cn=Blagg-NewsomeP]
Sent: Mon 4/13/2015 11:52:01 AM (UTC)
Subject: RE: Second Sight's final Part Two Report - your expertise required

Mark

The words look accurate.

Also we have investigated the number of sites in the pilot and understand that by the end of March 2010 there were approximately 550 sites installed.

Hope this helps.

Pete

Pete Newsome
Business Change Manager
Post Office Account, Fujitsu UK&I
Tel: [GRO]
E-Mail: pete.newsome@fujitsu.com [GRO]
Web: <http://uk.fujitsu.com>



Fujitsu is proud to partner with [Shelter](#), the housing and homelessness charity



Please consider the environment - do you really need to print this email?

From: Mark Underwood [GRO]
Sent: 13 April 2015 10:23
To: Harvey Michael; Kevin Lenihan
Cc: Newsome Pete; Patrick Bourke; Parsons, Andrew
Subject: RE: Second Sight's final Part Two Report - your expertise required

Hi Michael, if you could sign this off / tweak as required this morning. That would be great.

Thanks

Mark

Mark Underwood
Complaint Review and Mediation Scheme
[GRO]

From: Mark Underwood [GRO]
Sent: 11 April 2015 16:11
To: 'Harvey Michael'; Kevin Lenihan
Cc: Newsome Pete; Patrick Bourke; Parsons, Andrew
Subject: RE: Second Sight's final Part Two Report - your expertise required

Thank you Michael,

In terms of the first item – are you happy that the below tweaked wording is accurate and can be included in POLs reply to the Report?

- a. **Lack of token-based access to Horizon.** Horizon uses unique user passwords to control access to the system. If a user shares their user ID and password with another person, this cannot be prevented by software as there would be nothing to suggest to the system that anything untoward was occurring. Using a token-based access system is open to the same possibility of misuse as users could share tokens. User ID and password sharing is a serious contravention of procedure. Only a Subpostmaster is in a position to stop this happening.

Mark

Mark Underwood
Complaint Review and Mediation Scheme

GRO

From: Harvey Michael [GRO]
Sent: 09 April 2015 17:56
To: Mark Underwood [GRO]; Kevin Lenihan
Cc: Newsome Pete; Patrick Bourke; Parsons, Andrew
Subject: RE: Second Sight's final Part Two Report - your expertise required

Mark,

Our views are:

The lack of secure, token-based, user identification that would uniquely identify the actual user;"

It would be useful to have some context for this comment in order to give a more definitive answer. However, in any case, it is a matter of judgment as to the value gained versus cost incurred anyhow. For example, pre-HNGX there was a smart card (token) used by the Post Master to logon but this was used to log on at the beginning of the day. Therefore added little security benefit (for the cost) and therefore was removed when HNG-X was implemented. If one were to implement a token based approach such as we all use for personal banking then this would be more secure but it is only workable if you require ad-hoc transactions. If a Post Master was required to authenticate for each transaction then there would be a substantial impact on usability.

The unique user ID process that HNG-X uses fulfils the identifier requirement particularly if they are used in accordance with the stipulated process. Even if the unique identifiers are misused in the branch such that individuals are using ID's not allocated to them then we still are in a position to assert that the transaction did occur in the branch and this is all that we have ever done. We can tell you what ID was used when inputting the transaction but cannot (and have never sought to) assert that the individual who had the ID allocated to them was the person who inputted the transaction. It should be noted that even if tokens were implemented they would not remove this issue entirely as these could be shared too.

If the context is making reference to Fujitsu personnel performing transactions then the system still requires users to log on using their unique identifier and password. This identifies first and foremost that a Fujitsu person has performed the activity and secondly the individual themselves. We have no reason to believe and there has been no evidence provided that this process has ever been misused. It should be noted that being a IT company such user identification and password is part of our "DNA" process and as such is managed with appropriate rigour as part of our entire organisational processes. It should also be noted that we comply with all Post Office agreed security policies and that token based access controls were not stipulated as part of these policies. We are not sure of the benefit even if they were because surely the key insinuation that is being made (without evidence) is not with respect to which individual performed the activity but whether it was within the branch or not. The current approach provides evidence for this.

We have been told that, in some cases after a power failure, the main processor will automatically restart and commence the recovery process, but that the branch's screens will not automatically turn on. This means that any messages that are displayed as part of the recovery process, will of course not be visible to the user.

The simple answer is it can't happen. The recovery process is triggered by a user logging into the system after the system has restarted. There are some circumstances where the recovery is so simple that no user interaction is needed BUT even then my

original point holds true, recovery does not start until user has logged on.

Whilst I acknowledge that the report is highly confidential, it may be helpful to you for Post Office to share it with a limited number of individuals within Fujitsu such that we can provide appropriately contextualised input. If this would be useful we would put in a process to ensure it is shared only with named individuals.

Should you have any further questions or clarifications, please give me a call or send me an email.

Kind regards,

Mike

Michael Harvey

Commercial Director

Commercial, Legal & Assurance

Fujitsu

22 Baker Street, London W1U 3BW

Tel: GRO

Web: <http://uk.fujitsu.com>

From: Mark Underwood GRO
Sent: 09 April 2015 13:54
To: Harvey Michael; Kevin Lenihan
Cc: Newsome Pete; Patrick Bourke; Parsons, Andrew
Subject: Second Sight's final Part Two Report - your expertise required
Importance: High

Michael,

As Pete is away, could you please advise on the below. Second Sight has just issued their finalised Part Two Report. Within it they assert:

"3.13. Examples of inadequacies in Horizon's error repellency include: The lack of secure, token-based, user identification that would uniquely identify the actual user;"

And that in relation to lost transactions as a result of power cuts:

21.6. Post Office's position is that shortfalls cannot occur if the recovery procedures are correctly followed. It also states, in its response to the previously issued version of this report, that it:

"remains confident that branch accounts will not be corrupted due to power and telecommunications failures".

21.7. It incorrectly states, however, in that same document:

"This recovery process was reviewed in detail by Second Sight in their Interim Report and found to work".

21.8. The reality is, as we stated in our Interim Report, that we have established, from our investigative work, that the system may not have always performed as it was meant to after a reboot, particularly if a power failure occurred at the same time. We have been told that, in some cases after a power failure, the main processor will automatically restart and commence the recovery process, but that the branch's screens will not automatically turn on. This means that any messages that are displayed as part of the recovery process, will of course not be visible to the user.

Could you please write some words to rebut the assertions highlighted in yellow please. If you could do this today that would be fantastic.

Many thanks

Mark

Mark Underwood
Complaint Review and Mediation Scheme

GRO

This email and any attachments are confidential and intended for the addressee only. If you are not the named recipient, you must not use, disclose, reproduce, copy or distribute the contents of this communication. If you have received this in error, please contact the sender by reply email and then delete this email from your system. Any views or opinions expressed within this email are solely those of the sender, unless otherwise specifically stated.

POST OFFICE LIMITED is registered in England and Wales no 2154540. Registered Office: Finsbury Dials, 20 Finsbury Street, London EC2Y 9AQ.

Unless otherwise stated, this email has been sent from Fujitsu Services Limited, from Fujitsu (FTS) Limited, or from Fujitsu Telecommunications Europe Limited, together "Fujitsu".

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.

Fujitsu Services Limited, registered in England No 96056, registered office 22 Baker Street, London W1U 3BW.

Fujitsu (FTS) Limited, registered in England No 03808613, registered office 22 Baker Street, London W1U 3BW.

PFU Imaging Solutions Europe Limited, registered in England No 1578652, registered office Hayes Park Central, Hayes End Road, Hayes, Middlesex, UB4 8FE.

Fujitsu Telecommunications Europe Limited, registered in England No 2548187, registered office Solihull Parkway, Birmingham Business Park, Birmingham, B37 7YU.

This email and any attachments are confidential and intended for the addressee only. If you are not the named recipient, you must not use, disclose, reproduce, copy or distribute the contents of this communication. If you have received this in error, please contact the sender by reply email and then delete this email from your system. Any views or opinions expressed within this email are solely those of the sender, unless otherwise specifically stated.

POST OFFICE LIMITED is registered in England and Wales no 2154540. Registered Office: Finsbury Dials, 20 Finsbury Street, London EC2Y 9AQ.
