

Diane Martey

From: Mark Burley
Sent: 22 July 2010 11:55
To: Mike Young; Sue Huggins
Cc: Nick Beal; Philippa J Wright; Michele Graves; Mike Moores
Subject: RE: Urgent channel 4 horizon issuse

Mike / Sue

I have added some specific comments against the questions from David Smith below and would also note the following:

1. The point about the system being designed to retain integrity even when it fails is important as we could never claim, the system does not fail.
2. I am aware of 3 court cases - Cleveleys (Subpostmistress dismissed in 2001 - not long after Horizon introduced) (we settled out of court £187.5k as the expert for the SPMR produced a report which showed how Horizon could have caused the error. This could have been refuted with the audit trail but for some reason, this wasn't used / requested by our experts). Castleton where we presented a copy of the audit log to the Subpostmasters solicitor who promptly agreed there was no substance to the SPMR's claim and advised him to settle the debt. The solicitor was sacked by the Subpostmaster who proceeded to court, lost the case and liability of £300k but declared himself bankrupt. The judge decided there was "no flaw" in the Horizon system and "the logic of the system is correct" and "the conclusion is inescapable that the Horizon system was working properly in all material aspects". Alderley edge - £45k shortage (at audit) but judge dismissed case as unable to prove exact amount. However judge did not deem an investigation of the system was necessary (primarily it would appear as he deemed it would be costly and therefore not a good use of taxpayers money).
3. None of the Subpostmasters dismissed for discrepancies have - to my knowledge - produced any hard evidence. However in the past POL hasn't always tabled the evidence from the audit logs.
4. There are examples of human error discrepancies being 'rectified' several months / years later.
5. Computer Weekly ran an article in 2009 and another more recently picking up on the Justice for Subpostmasters Alliance (a group of Subpostmasters who are becoming more vocal about their claims that horizon has caused faults)
6. S4C ran a programme on the issue in 2009 (although I have not managed to see this)
7. There has been several flag cases over the years
8. There is a website - www.jfsa.org.uk - which has a lot of info and some cases. I think it would be useful to examine the cases and check up our position as we should be able to identify some of the actual people involved from the history on the case files.
9. I believe that the Group have a solicitor engaged who is working on a no win no fee basis (however I cannot substantiate this). I also believe there is an

22/07/2010

expert working with them who has requested information under the 'Freedom of Information (FOI) Act'. Again, I do not have any specifics on this.

10. My view - 3 reasons for shortage - Subpostmaster has hands in till; one of assistants has hands in till or (in most cases of a discrepancy) there is a human accounting error - some of which may be picked up over time.

Sorry there is a lot (especially with the extra bits below in red) - hope it helps. Happy to get involved in any other aspect, e.g. to help with point '8' above.

Mark Burley
Head of Projects (IT)
Banner St Wing
148 Old St
London
EC1V 9HQ

Tel: [GRO]

E-mail mark.burley [GRO]

-----Original Message-----

From: Mike Young
Sent: 22 July 2010 09:08
To: Mark Burley
Subject: FW: Urgent channel 4 horizon issue

Mark

FYI
Mike

Mike Young
Chief Technology & Services Officer
148 Old St, London, EC1V 9HQ

Tel: [GRO] Mob: [GRO] Mobex: [GRO]

-----Original Message-----

From: David Y Smith
Sent: 21 July 2010 19:04
To: Mike Young; Sue Huggins; Mike Moores
Subject: Urgent channel 4 horizon issue

All

Further to yesterdays complaint around horizon from oliver and a parliamentary question to ed davey from priti patel on the same issue we have today been notified tha c4 will run a news item on the same issue. This may be all the same group of people and may also just be a function of the new roll out. However.....

Sue Huggins will lead our response via Mary to the specific request. But I want an internal investigation under Mike Moores lead please over the next week on the following.

How robust is horizon?

Horizon is very robust against our Business rules but like any computer system it relies on accuracy of entry from the user although where possible controls are put in place to remove / reduce the risk of error. For example, if a transaction can only be sold in multiples of £5, then the system will not allow an entry of say £6. Additionally like any computer system, it can fail, e.g. in the event of a power cut. However the system is designed to retain integrity even when it fails. One of

22/07/2010

the key controls here is to allocate every transaction with a unique incrementing sequence number.

Once data is captured, data is replicated across all counters in a branch (a single counter position branch has two disc drives) and to the Fujitsu Data centre where it is again copied. Horizon does this once the 'basket is settled'. The system uses standard double entry book keeping, i.e. for every transaction, there is a corresponding entry against a method of payment.

In the Data Centre, a copy of the data is posted to the Audit file where it is retained for 7 years. Data in the audit file is sealed with a 'checksum' which is held separately to ensure that it has not been tampered with or corrupted.

Although the transactions are not committed until the 'basket' is settled, special rules apply to any transactions in the basket which have effectively already been committed such as banking and Automated Payment transactions. Again these are designed to maintain integrity.

Is it possible to mispost misallocate cash to the detriment of the Subpostmaster

It is possible to enter an incorrect value that ultimately results in a discrepancy when the Subpostmaster completes their accounts. For example, entering a bank deposit as £100 instead of £10 will result in the Subpostmaster recording a £90 loss (all other things being equal). As mentioned above, controls are put in place where possible to reduce or remove the likelihood of this. In some cases, an error like this will at some point be recovered but this depends on the type of transaction and potentially the integrity of the customer, i.e. with the banking deposit example, unless the customer declares the error, there is little likelihood of it being discovered and the Subpostmaster would be liable. An error of this type is no different to bank systems.

In summary the system will post the transaction as indicated by the Subpostmaster when manual input is required.

Where the transaction is fully automated, there is no evidence to suggest it could ever be misallocated. In theory it is impossible therefore (providing the Subpostmaster follows the instructions on the screen)

Is there any difference between horizon and hngx.

There are some significant difference in where data is stored (HNGx stores no data at the counters) but the principles around integrity remain in place as does the audit log. Importantly, when a branch migrates to HNGx it will have 2 audit logs - one for Horizon and a separate one for Horizon.

When hngx froze during the early trials is there any evidence that this caused misallocations?

There is no evidence this caused misallocations. However there is some evidence that branches may have had discrepancies as a result of not following the system prompts / instructions. Had they followed the instructions accurately, no branch should have had a discrepancy from a freeze. HNGx has been built as Horizon; namely to retain integrity even in the event of failure.

How do we treat discrepancies. Is there any exceptional circumstance applied where we don't seek recovery of funds prosecution etc. I.E are we heavy handed and disproportionate in our response.

How many subs have we terminated on this basis in the last ten years

How many have we prosecuted. What is our success rate?

As systems deployed
external assurance (most-
likely Horizon on-line)

What external audit verifications have been made of horizon and hngx

Need to understand
these

There have been a number of reviews of both systems by Gartner and other technology companies. I am not aware of one that explicitly focussed on integrity. However in addition testing of both systems has been extremely vigilant - over 25,000 separate and unique tests (many of which were run more than once) run over 18 months using approximately 8,000 mandays.

Horizon on-line

Review & testing

How difficult is it to rectify human errors to rebalance the till?

Ranges from very easy to not possible without external intervention.

What training does each user receive to use the system.

Originally users on Horizon received an extensive training course at the end of which they had to take a test which until they passed they would not be able to use the system (although almost impossible to enforce).

For HNGx, the majority of transactions and back office functions have not changed - the main changes are the User Interface and to a degree the Postal Services (although users have deemed this easier). We provide extensive pre go-live materials including web-site; training manuals, etc and then supplement this with an in-branch migration support on the day of and the day after migration. The Migration support will take the Subpostmaster through key areas and address any concerns. We have been measuring satisfaction with the training and support provided for HNGx and the following summarises the results to date (i.e. from start of pilot):

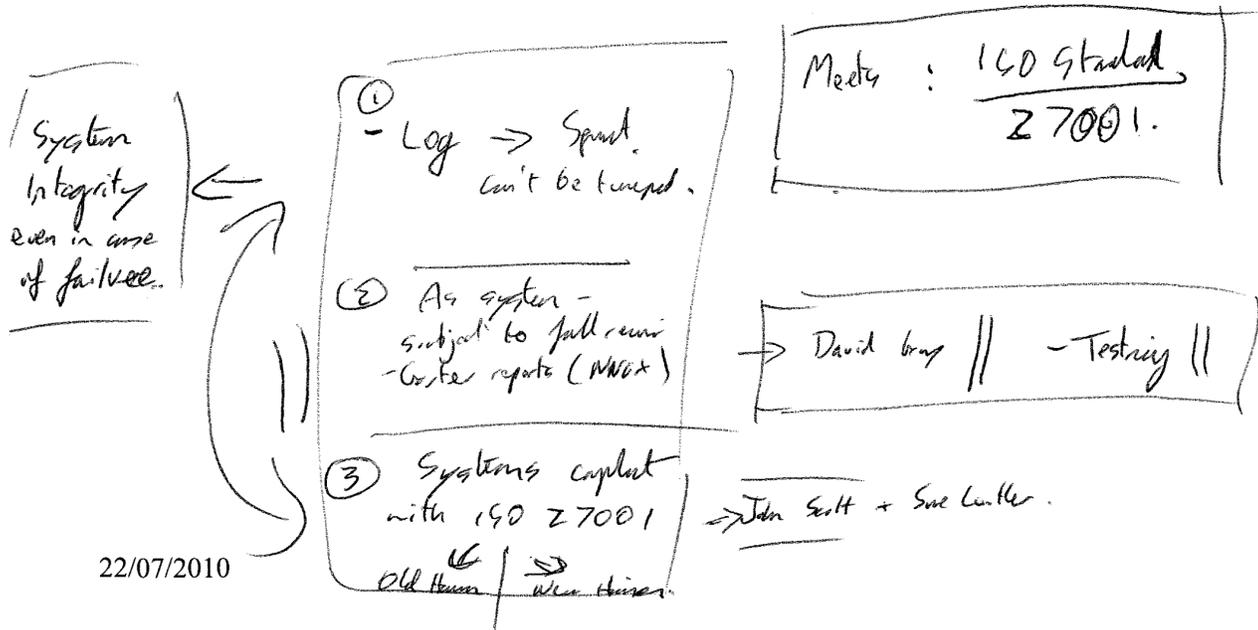
- 91% were happy they had the support needed during migration and that the training enabled them to adequately prepare for HNG

There is a facebook group of protestors online. What are they saying and what are we doing to ensure this does not harm the business?

Suggest we need input from lynn keith woollard rod and leslie as a minimum.

Thanks

Dave



- Audit Log.

- Each Txn check-sum basis

Revoke system

7 years

- Hold for



- rotating log lost

→ Old
Hardware
7 years

→ New
Hardware
data



- Txn/Evt

Audit

Log

→ Stores
records &
events

is a way this
needs

ISO

~~2700~~ 2700

IT Security Standard