To Dave Smith, Managing Director
Mike Moores, Finance Director
Mike Young, Chief Technical & Services Officer

From Rod Ismay, Head of Product & Branch Accounting

2 August 2010

Cc Mark Burley, Head of Projects (IT)
Lesley Sewell, Head of IT
Andy McLean, Head of Service Delivery
John Scott, Head of Security
Lynn Hobbs, GM Network Support
Sue Huggins, Head of Network Planning & Change
Mike Granville, Head of Regulatory Relations
Rob Wilson, Head of Criminal Law (RM Group)
Mandy Talbot, Principal Lawyer (Civil)
Keith Woollard, Head of Compliance
Michele Graves, Executive Correspondence Manager

Horizon – Response to Challenges Regarding Systems Integrity

Post Office Ltd has, over the years, had to dismiss and prosecute a number of subpostmasters and Crown staff, following financial losses in branches. A small number of these have made counter claims that they were not guilty of the charges made but that the Horizon system was faulty.

Various lobby groups have been set up by former subpostmasters and these have at times received national media coverage and in some cases been taken up by local MPs. Most recently, Channel 4 has proposed a news article about this area.

This paper has been compiled as an objective, internal review of POL's processes and controls around branch accounting. It includes an overview of

- POL's control environment and POL's response to accounting errors
- IT systems – Horizon versus Horizon Online and resolution of known issues
- Third party perspectives – Court judgments, media and audit
- Statistics on branch accounting issues, suspensions and prosecutions

Executive Summary

The allegations to which we are responding follow on from cases where thousands of pounds were missing at audit. We remain satisfied that this money was missing due to theft in the branch – we do not believe the account balances against which the audits were conducted were corrupt.

POL has extensive controls spanning systems, processes, training and support. Horizon is robust, but like any system depends on the quality of entries by the users. Horizon Online builds on this and brings benefits to running costs and change management. It is not being done because of any doubt about the integrity of Horizon.

The integrity of Horizon is founded on its tamper proof logs, its real time back ups and the absence of "backdoors" so that all data entry or acceptance is at branch level and is tagged against the log on ID of the user. This means that ownership of the accounting is truly at branch level.

Subpostmasters are trained to use the system, they have support material in branch and there is a wealth of helpline support available. Some transactions and processes could be made more intuitive, but the support is there for queries.

Accounting errors do happen through user mistakes, but these can be explained and resolved case by case. Systems issues have also arisen but again POL has been able to explain them and rectify them. Whilst they have affected the availability and functionality of the system, with consequent impacts on customers and clients, they do not bring the integrity of the system into question.

When POL takes a subpostmaster to court we have strong processes for the compilation of evidence, compassionate factors are borne in mind and we have a high success rate. This does depend on ensuring that the courts focus on the facts of transaction logs and not on speculation about the "what ifs".

There are several improvement opportunities for POL and these are set out in Appendix 1. They do not undermine POL's assertion regarding the integrity of Horizon, but they would tackle some of the other noise which complainants feed on. They may also help when POL does take action.

1. POL's Controls

POL has extensive controls within Horizon and in the communication of branch accounting records to the central finance systems (primarily the POLFS system). POL also has clear processes for the recruitment and training of staff and for access to support services such as Helplines.

1 (a) Systems

The independent IT consultancy Gartner has described the Horizon Online architecture as first rate and the existing Horizon system has had positive press. Horizon and HOL were both designed with the principle that only authorised branch users can create or accept transactions in the system. Robust security is an important and integral part of the design and management of both systems.

Failures in systems and file transfer do happen, but POL has controls to detect these. The frequency of file transfer failures has been unacceptably high recently and is a top priority for IT

The system depends on the quality and accuracy of data entry by users, and on branches controlling the permissions levels that they grant to their users. POL has enabled controls at a branch level for the prevention and detection of errors and these are supplemented in P&BA.

Hardware and software development, installation, enhancement and maintenance

- Change management – formal processes and decision points with authority levels
- Extensive testing including user acceptance tests
- Trained engineers on site and with requirements for proof of ID when working

Physical Access, Systems Users and log-ons

- Physical security processes for branches to prevent unauthorised staff on site
- Leaver / joiner controls for allowing and removing access to Horizon
- All users require log on IDs and passwords
- The person in charge in the branch can set the appropriate levels of access for different users
- All transactions and events are tagged and traceable to the user
- Security is designed and managed in accordance with respected national and international standards such as ISO / IEC 27001. It is subject to regular independent audits

Transaction automation – minimising manual entry / choice and enabling validation of entries

- Use of cards, tokens, barcodes and system reference data to minimise manual data entry
- Cash centre automation and CCTV in the event of branches disputing cash rems (England only

Business continuity and systems recovery

- Alerts for failed transactions in branch and centrally eg. for power cut or severed lines

Transaction recording, back up and proof against tampering

- Sequential referencing of transactions, customer baskets and associated user IDs. Prevents gaps, duplication or anonymous transactions
- Transaction back ups – back up server updated as each transaction is completed
- Audit file and "read only" control – transaction records securely sealed
- Events such as branch balancing are also securely recorded and are traceable
- System drives double entry accounting and ensures it remains in balance

Interfaces to central finance systems

- Automated interface checklists, batch schedules and exception reports
- Batch controls ("BLE" and "BIMS") between branch, middleware and finance systems
- Non polled reports if no data is received from a certain branch
- SAP system and middleware – daily checks for stuck data and for exceptions (iDocs)
- Reconciliation and alignment of different data feeds – eg. between data to clients and to POL

1 (b) Processes

Accounting and control in branch

"Accurate accounting is not difficult for well run branches" – the systems and support are in place for branches to maintain comprehensive, accurate and timely accounts, and transactions can only arise in Horizon from actions of the subpostmaster or their staff.

Branch accounting is included in induction training and support is available in service.

Horizon operates on a "double entry" accounting basis and maintains a balanced trading position. Staff are then responsible for ensuring that they record transactions and methods of payment promptly and accurately. They have the tools, and they are encouraged to do physical checks.

Mistakes do occur (intentionally and unintentionally) and this is where supervisory checks are important in the branch and where detection processes from central teams would come into play.

Balancing routines

- Daily cash declarations – an event where staff at each till position count and report their physical cash holdings and Horizon then flags up any difference compared to the system
- Cut off routines (daily and weekly) – for onward submission to P&BA / Clients / Suppliers
- Weekly Balance Period Rollovers – a full check and declaration of all branch assets and comparison to trading records. Discrepancies can be ringfenced for resolution in suspense
- Monthly Trading Period Rollover – as above but requires the discrepancies to be resolved either by putting cash in or "settling centrally" to a debt ledger managed from P&BA
- Branch Trading Statement, physical signature and retention – a monthly requirement
- Other control reports in branch eg. Balance Snapshots, Transaction Logs, Suspense Reports, Daily Sales, Reversals etc. These help identify errors and internal fraud and are available to subpostmasters at any time

Transaction capture

- Automated products – cards, tokens and barcodes force a transaction into the system because the clerk has to scan or swipe something
- Matching routines for stand alone kit – branches may forget or make mistakes in recording transactions at kit such as the ATM, Lottery terminal or PayStation. P&BA get a feed from the terminal to compare to Horizon and alert the branch to errors / omissions
- Balancing routines to detect omission of stock sales – physical stock checks spot these

- Cut off routines to detect omissions or misclassifications of vouchers encashed and methods of payment accepted – the control is the physical match against the system
- System reference data – eg. postage and travel insurance have embedded price tables

IT systems interventions and response to outages / disconnections

- Incomplete transactions – systems could fail or lines could be disconnected during online banking transactions. This could mean that customer money has changed hands without the system being updated or vice versa. IT controls would detect these outages and raise recovery alerts to the branch such that the branch can check and update the accounts if needed. This has been a more frequent issue recently with "screen freezes" and "POCA outages" but recovery instructions have been issued to branches to enable them to deal with any issues

Independent checks in branches

- Around 2,000 branch audits are conducted each year, driven by risk model
- All branches are receiving a high level cash count during migration to Horizon Online
- Area managers may from time to time enquire about branch accounts during visits

Accounting and control in P&BA

Central controls over accounting are primarily in the Product & Branch Accounting team (P&BA) but also include activity in cash centres and alerts from our method of payment processors.

P&BA has initiated a turnaround time commitment with Network for prompt notification of errors to branches. P&BA has also worked closely with the NFSP ET on tone of voice and constructive service as well as robust intervention in the accounting arena.

P&BA tracks its delivery and its accounts accuracy through interface alerts, reconciliation of data streams, a focus on prompt resolution and various checks on individual account balances.

Complete, timely and accurate data feeds

- Joint working and alerts with IT teams in respect of expected interfaces, batch routines and any incidents of data getting stuck in transmission
- Reference data and account mappings – these are secured in the system and there is segregation of duties around changes

Data matching

- P&BA data matching – comparison of stand alone branch terminal data against entries in Horizon (for ATM, Camelot, PayStation, Sodexho Asylum Seekers, Post & Go)
- A&L paper matching – comparison by A&L of paper vouchers sent in by branches against Horizon daily and weekly summaries
- Cash and bureau in transit matching – checks of what branches recorded as sent or received compared to what cash centres recorded
- Cheques in transit – comparison of what branches reported as sent against what the cheque processor physically receives
- Matching routines – automated routines with defined parameters and rules

Error resolution

- Thresholds and policy – P&BA operates a "maintained error" policy whereby differences below defined values are written off and not investigated further on certain products
- Client enquiries – issues of completeness or timeliness of data files may results in amendments to data in POL systems or client systems
- Customer enquiries – response to ad hoc queries received at P&BA and Customer Care
- Branch ownership – branches are advised of issues and referred to Operations Manuals
- Judgmental write offs and authority levels – P&BA has defined authority levels for write offs and requirements for rationale which would not set adverse precedents in branches
- Transaction corrections – "double entry" adjustments sent to branches for their acceptance. There is no "back door" to force them into branch

accounts. Visibility is key to ensure ownership of the issue and prevent any risk of arguments about "back doors"

- Dispute process – this has been communicated to branches whereby transaction corrections and discrepancies may be challenged by any branch
- Prompt response – the commitment with Network is for 95% of issues flagged within 3 months, but in practice most are soon after 1 month and some key ones are next day

Account reconciliation, probity and audit

- Individual accounts are subject to reconciliation with checks against expectations and supporting evidence
- Reconciliations are also subject to external audit
- Internal audit reviews are conducted each year on "Critical Business Processes" and these have covered some processes within P&BA

The interaction of P&BA, Network, Audit, Security and Legal

P&BA is in the front line of detecting suspicious activity. This fits well as an aspect of managing and assuring client, branch and bank balances.

P&BA works closely with colleagues in other directorates and has clear escalation channels for alerting about any systems or process issues, for proposing themes for fraud risk models and for highlighting individual branches were a surprise visit by auditors or investigators may be needed.

P&BA also works closely with the civil and criminal law teams in the support of court actions.

Conformance and Fraud Risk monitoring and intervention

- Accounts checks based on past experience of poor conformance and fraud routes
- Prompt dialogue with branches enforcing the awareness that P&BA are watching
- Joint working groups with Security etc – eg. Fraud Forum and Losses Group
- Joint work with Cash Services on unusual cash trends and postings in branches
- Cash delivery and collection optimisation to minimise the scope for theft in branch

Debt Recovery

- Visibility of issues in branch – anomalies in the accounts or in physical stocks are visible from standard reports and basic stock counts. This creates a foundation for ownership
- Acceptance of debt by the branch – branches do actively choose options in Horizon
- Contractual responsibility for losses – this is clear in the subpostmaster contract
- Enquiries and transaction corrections – branches are informed of issues to enable to them prevent future recurrence of the same themes
- Statements and reminders – there are clear processes and milestones for reminders
- Repayment schedules are agreed with Network management and with sensitivity to financial hardship of the payee

Suspension and follow on

- Auditors have defined processes for their tests in branch and defined escalation routes
- Decisions not to suspend an agent require authority on a tiered basis within the Network

Legal action

- When discrepancies are identified, the case goes to Investigations to decide whether there is a criminal case to be pursued
- Decisions on taking civil or criminal action involve qualified legal experts
- Qualified decisions are made as to pursuing a specific debt under "theft" in the criminal court or pursuing "false accounting" where the value awarded can involve the judge
- Court proceeding are driven by the Legal Team
- Decisions not to continue legal action, to resolve out of court or to write off are taken with informed authority and consciously with a view to not setting a precedent
- Decisions do take a variety of circumstances into account including compassionate factors as well financial cost / benefit. We consider POL errs more to the compassionate side than the draconian side in its legal actions
- Criminal prosecutions are not based on cost / benefit. As a "Prosecuting Authority" Royal Mail has to ensure a consistently robust treatment of crime not based purely on value
- Standard approach to statements for court including what should have happened and what actually happened

1 (c) Recruitment and Training

Agents are recruited based on business cases, credit checks and behavioural interviews. Agents are then responsible for the recruitment of their own staff.

Further induction controls and subsequent monitoring of agents in service were considered within the Network Efficiency Programme but could not be progressed for legal reasons.

Training is provided to Subpostmasters at induction. They are then responsible for onward training of their own staff. Subsequent training or communications happen when significant new products or processes are deployed. . Branch staff are also required to take and pass appropriate compliance checks to comply with legislations e.g. relating to Financial Services.

Training and targetry have increasingly focussed on sales. Whilst regulatory compliance has rightly had more airtime there may be a need to reinforce awareness of the key accounting routines in branch and to facilitate more of a "self help" model with greater accountability.

1 (d) Support

Support is available to branches through 3 main channels – Operational Instruction manuals, the Network Business Support Centre (NBSC) and Network line management.

Over time, however, branches have accumulated contact points in many parts of POL and in suppliers and clients. This has therefore undermined the consistency of support. A project is under way within Service Delivery to clarify "Single Point of Contact" and this will be a helpful step.

Network Business Support Centre (NBSC)

- A tiered helpline which can refer callers to more specialist support lines. The NBSC operates 8.15am to 6pm (Monday to Friday) but extended to 8pm on Wednesdays where more accounting support is required, and 8.30 – 2.00 on Saturdays. Emergency support such as for Security is available 24/7.
- The NBSC has a knowledgebase of standard guidance to advise branches (which is generally the same information that branches have in their support manuals). The knowledgebase has been updated for Horizon On Line and has received praise from recent independent reviews.
- The NBSC will refer specific calls and trends to expert domains such as P&BA for accounting or Fujitsu for software issues.
- The NBSC have weekly operational review meetings with Fujitsu's Service Desk.

Suppliers

- Branches have contact numbers for various suppliers for technical support (hardware/software issues). Some of these are options off the NBSC call plan.
- Whilst branches sometimes stray into accounting queries whilst on the phone, we always instruct suppliers to refer the branch back to the NBSC.

Suppliers

- Branches have contact numbers for various suppliers. These may be for engineering matters but can stray into accounting eg. with Wincor Nixdorf on ATMs

Reference material

- Counter Operations Manual – paper based file with monthly updates for insertion
- Horizon Online Help – the incoming replacement for the paper based operations manual
- Operations Focus – weekly updates and guidance on transactions and services
- Memoview – messages direct to the Horizon terminal
- Various magazines which may include "training content" eg. SubSpace

2. IT Systems

Horizon

Horizon was developed as an electronic point of sale to replace archaic paper based accounting processes. It utilised hardware in branches which had strong security features and interfaces to a central data centre with high security. Data was replicated between units in the branch and once it reached the central data centres it was replicated between those.

This gave three strengths which are important in terms of the allegations being made:

1. Horizon infrastructure was robust from a security and access perspective
2. It was resilient in terms of being able to continue customer service and to hold data in a queue in the event of incidents, and
3. It had strong back up and integrity features with data backed up in branch and centrally

This provided a strong audit trail. Further narrative from Fujitsu is included at Appendix 3.

Horizon v Horizon Online (HNG)

Horizon Online has been designed to give the Business Equivalence of Horizon. It has been driven to reduce costs by having the system on a central data store rather than being managed by end of day data collection from individual branches. Horizon Online is made up of a combination of new and migrating components.

Counter

- No data stored locally, all data is stored centrally on Branch Database
- System in now completely online so it is not possible to transact without connectivity to the data centre
- Solution uses existing equipment in Branch (base unit, keyboard, screen pin pad, scales etc)

Router

- Improved backup connections using the mobile network
- New Branch Router to allow discrete counter connection to data centre without reliance on Gateway PC

Network

- Secure VPN's used to connect to data centres

Data Centre

- Infrastructure now located in state of the art datacentres in Belfast
- Bladeframe infrastructure provides faster, more reliable infrastructure
- Full resilience - solution is n+1 (ie additional capacity to allow for failures)
- Storage and backups are faster and more resilient spanning data across the two data centres

Security

- No data held locally in Branch
- Vulnerability scanning, reporting and patching systems. Intrusion Detection/Prevention systems in key areas.
- Segmented architecture with firewalls and routers protecting traffic in and out of sensitive domains including cardholder environment

3. Known IT Issues and Their Non Applicability to the Allegations Made

(a) Screen Freeze / Recovery

Many Horizon Online branches have been frustrated by system outages. The root causes have been clarified and resolved and this is evidenced in the accelerated rollout.

Branches were frustrated when they could not serve at all, but were also concerned about accounts integrity when transactions were cut of in mid-flow.

However, transaction alerts were in place and revised operational instructions have now been issued to enable branches to complete or to cancel the accounting entries dependent on whether they physically completed the cash transaction with the customer. Further detail is included at Appendix 4.

(b) Barcode Sticking

A small number of branches have experienced a situation where a customer transaction (eg. a bill payment) sticks on the details of the preceding transaction. In some cases the branch has spotted it immediately but in some cases it has only come to light when the customer complains that they are being chased for an "unpaid" bill. Incidents go back to 2005.

Up to now it had been understood that it related to a version of scanners where POL did not know which other branches had the same version. It was not therefore possible to isolate other branches. It was also a rare event on the scanners themselves. It was not a systematic failure with every transaction on the particular scanner.

Fujitsu have investigated this and now advised that it is not hardware related – it is a Riposte software issue. It will cease to be a problem with Horizon Online, as HOL does not use Riposte.

This issue does not appear to have arisen in any of the legal cases in question and the incidents have been resolved at all the branches where it has been noted. This is not considered a systematic integrity issue for Horizon and it should be resolvable from the facts of records in the Horizon transaction logs.

(c) Non Polling

Small numbers of branches fail to poll due to issues such as telephone lines being dug up. The system holds the data in a queue so this does not undermine integrity. It just affects the timeliness of data, and this is catered for in decision making by P&BA. The issue goes away with Horizon Online as the data store is online not in branch.

(d) File delivery failures

These do not affect branch records but have meant P&BA and clients may not have received a days transactions. This is a priority fix for IT, but carries a PR risk.

(e) Horizon / POLFS differences

In 2005, P&BA moved onto a SAP system (POLFS). This was an exceedingly complex IT migration and there were some issues in management of the cut off which meant P&BA was out of synch with some branches in terms of opening balances for cash and bureau. This did not affect the integrity of Horizon and has been catered for in error resolution with branches, but it has affected service to some branches ie. Where decision making on cash supply was based on wrong data centrally. Some issues have continued to come to light recently but this is now under control. It is not relevant to the allegations.

4. Third Party Comment – Court Decisions, Media and Audit

4. (a) Court Decisions

There have been cases, when taken to court by POL, where the defence has claimed that the accounting system Horizon was at fault and that there were incidents such as "ghost transactions" or "electrical supply issues" which have corrupted the Horizon records.

With 2 notable exceptions, POL has been able to rebut these assertions by ensuring a focus on the facts of the Horizon transaction logs and a request for the defence to be specific about which transactions they consider to be "ghost" and why.

Since 2005, which was the start of the existing case management system, there have been 382 Criminal Law cases forwarded for legal advice of which 230 proceeded to court. Of those 169 have been found guilty and 18 defendants cautioned. Of the remaining 43, 1 was found not guilty but this was nothing to do with any Horizon challenge and 42 cases were not carried forward. There is no suggestion in any of these 42 that POL had any concerns itself about Horizon – the decisions not to proceed included compromised passwords preventing a case against the individual, "not in the public interest" such as where there were medical issues, decisions by the Procurator Fiscal not to proceed (which he need not narrate) and inability to identify the suspect.

There are three "landmark" cases which feature in the arena of challenges to Horizon.

1. B055 (2001) – subpostmistress dismissed in 2001 soon after Horizon was introduced. The defence produced a report which showed how Horizon "could" have caused an error and POL did not have the audit transaction logs to refute the claim. POL settled out of court for £187k, but subsequently improved the retention of audit transaction logs. This case would not have the same outcome today because of improved liaison between Fujitsu and POL and availability of logs.

2. B009 (2004) – B009 claimed that Horizon was faulty and found other subpostmasters to back him. However, POL presented the audit transaction log to his solicitor who promptly advised B009 there was no basis to his case. B009 sacked him, lost the case, was found liable for £300k and went bankrupt. The judge decided there was "no flaw" in the Horizon system and said "the logic of the system is correct....the conclusion is inescapable that the Horizon system was working properly in all material aspects". This case appeared to have put a stop to allegations, however, B009 has continued to promote lobby groups, assisted others to find no win no fee laywers and remains vocal in the press. Various publications have in turn quoted him,

but we have made a strategic decision across the group so far to quietly respond to each individual rather than mount a pro-active PR campaign.

3. Alderley Edge (2010) – The subpostmaster, A012, did plead guilty in [redacted] Court to false accounting, but POL had initially pursued him for theft and had to reduce the charge to false accounting due to printer issues with the legibility of branch trading reports. Press comment has focussed on certain comments by the judge. The judge said he had issues with the proof of size of the loss and also said "there are issues relating to the Post Office computer system which I do not feel able to judge". Critics of Horizon therefore focus on these comments rather than the fact that A012 pleaded guilty.

In summary for POL, the record of prosecutions does support the assertion that the subpostmasters have been guilty rather than that Horizon is faulty. However, this does not stop speculation about the system. It is not possible to stop people saying "..what if.."

There have been no cases challenging Horizon Online yet, but POL remains as confident about the integrity of HOL as it does about Horizon. IT Security have also reviewed incidents, with no common theme or trend arising such as to confirm an integrity issue.

4. (b) Media

Media and public discussion about Post Office systems has included:

1. TV – S4C's "Tara Naw" programme in September 2009. This included similar individuals to those involved in the current internet groups. Welsh MP David Jones was proposing a Commons debate about Post Office IT systems on the back of it. Comments were made by NFSP ET which were supportive of POL but these were not included
2. TV – Channel 4 continue their investigations and had proposed a main news slot
3. The Grocer magazine – various articles linking back to [redacted] B009
4. Computer Weekly – links to articles including "MP seeks answers over Post Office IT systems", "Post Office slammed by MPs over Horizon system" and "Bankuptcy, prosecution and disrupted livelihoods – Postmasters tell their story". This in turn led to discussions with MPs to rebut the suggestion that POL was delivering Horizon Online as a cover up to tackle errors in the basic Horizon system
5. Accountancy Age – similar comments and suggestions from "IT experts" that POL should get an independent review commissioned
6. Internet – "Justice For Subpostmasters Alliance (jfsa.org.uk)" and "Postofficevictims.org.uk"

To date, POL has ridden the wave of press comment but chosen not to pro-actively mount our own media campaign.

4. (c) Independent Review and Audit Angles

POL has actively considered the merits of an independent review. This has been purely from the perspective that we believe in Horizon but that a review could help give others the same confidence that we have.

Our decision between IT, Legal, P&BA, Security and Press Office has continued to be that no matter what opinions we obtain, people will still ask "what if" and the defence will always ask questions that require answers beyond the report. Further such a report would only have merit as at the date of creation and would have to be updated at the point at which Horizon or the numerous component platforms were upgraded.

Ernst & Young and Deloittes are both aware of the issue from the media and we have discussed the pros and cons of reports with them. Both would propose significant caveats and would have limits on their ability to stand in court, therefore we have not pursued this further.

The external audit that E&Y perform does include tests of POL's IT and finance control environment but the audit scope and materiality mean that E&Y would not give a specific opinion on the systems from this.

It is also important to be crystal clear about any review if one were commissioned – any investigation would need to be disclosed in court. Although we would be doing the review to comfort others, any perception that POL doubts its own systems would mean that all criminal prosecutions would have to be stayed. It would also beg a question for the Court of Appeal over past prosecutions and imprisonments.

The reviews and audits that are currently conducted include an annual LINK security standards audit which has been satisfactorily signed off. Future audits will include PCI DSS (Payment Card Industry Standards) and ISO27001 Certification (covering data centre operation from the start of HOL and the whole of Fujitsu's HOL service from any day now)

4. (d) Allegations on websites and in magazines

Comments on the "Justice For Subpostmasters" site (Jfsa.org.uk)

After years of being forced to suffer in silence, the injustices that have been forced upon many Subpostmasters by the Post Office are being exposed across the country. No longer will the Post Office be able to hold a financial gun to the head of a Subpostmaster.....

....."The problem is that the Post Office Horizon system is so flawed that nobody knows how to fix it, but in the meantime subpostmasters are continuing to be made to suffer."

.....JFSA has access to IT experts, forensic accountants, a criminal law firm and a major national firm of solicitors who are acting for us in civil matters.....

- There has to be an independent investigation into the introduction, operation, reliability and accuracy of Horizon.

- A complete change in the way subpostoffices are managed by the Post Office. Together with a new and fairer contract for subpostmasters that removes the pin-head dancing around a subpostmaster being an agent or an employee. A new contract that actually covers the use of IT in subpostoffices.

- An ombudsman or an independent third party has to be introduced between the Post Office and the subpostmaster who would hear appeals in issues of disagreement, as currently the Post Office act as judge, jury and executioner.

- Finally, the removal of the cosy relationship between the Post Office and the Federation has to happen (described by many as when the Post Office says jump, the Federations only answer is, how high). This could easily be achieved by establishing an extra and alternative representative subpostmaster body.

Response to these allegations

Independent investigation
Third party experts have been involved in Horizon's design, test and rollout. Subpostmasters have been involved in defining requirements and in user acceptance testing. We do not consider a report necessary. Even if one were produced, it could not prevent speculative "what if" questions.

Subpostmasters Contract and NFSP Relationship
These are not relevant to the integrity of the system.

Independent Appeals

POL gives considerable resource to hearing both sides of the argument. Our history of write offs supports the view that we are sensitive. Our success in court cases does not suggest an independent appeals process is needed

Other common challenges include:

"Ghost transactions"
Horizon has secure access controls, transaction logs and no back doors. All transactions are initiated or authorised in branch. No defendant has yet identified and substantiated a "ghost transaction"

"Horizon did not let me access the records of all transactions recorded against my branch"
Horizon does have transaction logs which are accessible in branch. Transaction corrections issued by P&BA are also visible on receipt and for later enquiry in the branch.

5. Branch Accounting Issues – Most Common Issues and Work to Tackle Them

POL conducts around 80 million customer sessions and 230 million transactions per month, in the service of around 700 corporate and governmental clients. This is delivered through 35,000 counter positions across its estate of 12,000 branches. On a typical day this results in the central finance team settling £175m to clients and tracking the clearance of £100m of cheques and cards.

In 2009/10, P&BA issued 153,000 transaction corrections (TCs) to branches (down from 165,000 year on year). Several of these were in turn a consolidation for a month of a sequence of daily accounting errors by a branch. The most common themes for TCs were:

Type	% of total	Volume	Proposed solution
Caused by branch			
Camelot	31	48,283	"Ping" automated data feed
Cash rems from branches	11	19,994	Branch conformance reminders
A&L banking and Giro cheques	8	11,863	Branch conformance reminders
Cheques sent to EDS	6	8,585	Branch conformance reminders
Aon	4	5,694	Pricing automation rolled out
Bureau	4	5,410	Branch conformance reminders
PayStation	3	4,423	"Ping" automated data feed
Other	18	27,331	
	85	131,583	
Not caused by branch			
ATM retracts	5	7,864	Branch awareness of retracts
Cash rems to branch	4	5,426	Cash centre conformance
Stock rems from stock centre	2	3,833	Stock centre conformance
Other	4	4,957	
	100	153,663	

Branch errors included under and over statement of transactions and the omission of activities of both a deposit and a withdrawal nature.

The average value of a TC to credit cash balances was £546 and the average for a credit was £527. Many individual TCs were small, but some such as banking deposits where the transaction was miskeyed with too many zero's could be in the hundreds of thousands of pounds.

The decision to issue small value TCs is based on giving the branch the comprehensive view of all their accounting issues and that it is more cost effective for P&BA to automate the whole run rather than separate out low value items. The NFSP have been supportive of this approach.

Whilst it is undesirable for this level of errors and corrections, the wider evidence does not suggest a problem of data integrity or a systematic failure in systems or processes. The correction level is less than 0.01% of the underlying 230 million transactions per month. Furthermore the majority of branch audits are satisfactory.

Turnaround times for notifiying issues to branches are underpinned by an agreement with the network for 95% of issues to be notified within 3 months. In practice P&BA is well ahead of this and key issues (eg. cheque despatch concerns) would get intervention as fast as next day. The agreement caters for branches monthly trading processes (and a cost/benefit decision to let timing issues wash through rather than flag them all during the month). The slowest notifications would arise where we are dependent on a customer to flag the issue – eg. a keying error on a bill payment.

P&BA is working with Marketing and Operations to design out the scope for error where possible, but this is not a short journey.

TCs are not an indicator of systems integrity issues. They are a reflection of poor adherence to defined processes. Nevertheless the underlying errors create noise in the system and an environment where it is easier to make the broader allegations.

6. Branch Audits and Outcomes

Branch audits are driven by a risk model which has taken input from relevant teams across POL. Cash audits are also specifically being done as part of the Horizon Online migration. These latter are not full audits, but they would be expected to flush out situations where a significant amount of money was missing.

The overall audit results for the last 4 years are as follows:

			Reason for Suspension			
Period	Audits	Agents suspended	Audit shortage	Bankruptcy / Administration	Property	Other (POCA/ Police Action)
2007/08	1685	190	184	1	3	2
2008/09	2326	229	217	4	1	7
2009/10	2303	214	199	1	3	11
2010/11 (Apr to June)	458	41	37	0	3	1

			Outcome				
Period	Audits	Agents suspended	Summary Termination	Resigned to Avoid Termination	Reinstated	Died during period of suspension	Case not concluded
2007/08	1685	190	94	60	36	0	0
2008/09	2326	229	117	53	56	3	0
2009/10	2303	214	94	72	48	0	0
2010/11 (Apr to June)	458	41	17	9	6	0	9

Losses in branches can be caused through several reasons, but the most common is typically the theft of cash and the subsequent cover up by falsification of accounting balances. The approaches and detection mechanisms include:

Approach	Detection Mechanism
Falsely declare cash balances – eg. branch has £40k, staff steal £10k but continue to declare holdings of £40k	• Tighter (lower) cash holdings give branches less scope to falsify cash without having to appeal for more deliveries • Monitoring of unusual trends in cash balances • Branch audit
Falsify value of cash sent to cash centre	• Checks on contents at the cash centre (under CCTV in England and supervised in Scotland)
Journal between cash and cheques in branch, then claim to have sent cheques to EDS for processing	• Daily matching of cheques despatched by branches compared to receipts at EDS
Claim that customers paid by "savings stamp" and that the stamps were sent off or lost	• Checks on returned stamps at Chesterfield • Current migration of stamps to budget cards
Falsification of inpayment and	• Favoured products have gradually

outpayment transactions and values	been eliminated by automations • Remaining items such as "Giro cheques" are checked by A&L and evidence returned to us where gaps arise between point of sale summary and physical "cheques" sent in

Issues can arise in branch cash balances due to inadvertent keying errors by the branches. The branch auditors would check this out with P&BA before getting to a point of proposing suspensions and terminations.

Appendix 1 – Improvement Areas

Branch awareness and ownership / accountability

1. Branch training – to raise awareness of key Horizon reports and scope for self help
2. Absentee managers – to identify and address absentee subpostmasters and managers
3. Ownership and accountability in branch – to improve the standard of ownership
4. Password security – local commitment to not sharing passwords and to locking keyboards when away from the counter (could be built into Subpostmasters contract)
5. Prioritisation of conformance and accounting in the supervision and targetry of branches
6. Cash remittances – better conformance by branches in making up contents of rems

Single points of contact and speed of turnaround

1. Single point of contact – to rationalise and communicate contact points for branches
2. Incident response – to improve response times and clarity of ownership

Readiness for court, focus on facts and strategy for dealing with public allegations

1. Single accountability – for co-ordinating and responding to challenges and allegations
2. Court cases – to ensure consistent use of Horizon transaction logs and explanations. To include the resourcing point between criminal and civil prosecutions
3. Consider contract change with Fujitsu to increase access to "ARQ transaction logs" and whether POL uses its contractual allowance for the right priorities
4. Learning points from the Alderley Edge case – care when amending a plea from theft to false accounting. Even where a defendant has pleaded guilty to ensure that allegation that POL has suffered no loss can be refuted at Court
5. Case management system – to give single view of records between P&BA, Network, Legal, IT, Service Delivery and Security
6. Press comment – to reconsider our media stance in light of past court case outcomes
7. Pro-active briefings – ensuring key stakeholders do understand the facts
8. Review strategy for response to allegations and speculation

Plain English instructions

1. Processes and instructions need to be clearer and punchier

Systems

1. Client file delivery and online services – to complete the improvements under way
2. Software code changes and proof of authorisation – to improve the sign off process and documentary evidence of sign off. This has been a criticism in the 2009/10 external audit. It did not apply to Horizon, but was a theme from reviews of Credence change control
3. Manual transactions – continued automation and greater use of user entry checks
4. Cash remittances – automation of Scottish centres to same level as England
5. Stock remittances and accounting – to improve tracking between branch and stores and to make branch recording easier

Process and control documentation – improving accountability and version control

Balance of firmness and compassion

1. Benchmark POL suspension and prosecution rates against other retailers
2. Continue acknowledging hardship but could fairly charge interest on debt

Minimising opportunity – keeping cash down and closing enquiries quickly

Internal Audit – consider alignment with existing Critical Business Process and Control reviews

Appendix 2 – Current Cases With Possible Challenges to Horizon

Criminal Law Cases

As of April there were 12 live cases where it was thought the defence team were challenging the integrity of Horizon. Case notes are below. In several cases these do beg a larger question of "where is the cash" rather than "what could be wrong in the data". It will be important that POL and Group marshall our resources to ensure a robust and consistent approach to responding to these criminal cases as well as to the other population of civil cases.

Post Office	Date	Loss £k	Other pertinent information(i.e. magistrates comments or external audit done)
Newsome	2005 to 2008	169	A211 confirmed that his normal cash holding figures were in the region of £40,000. He then stated that due to a number of Horizon technical problems he had not been paying money out to customers and had therefore generated a build up of cash. Forensic Accountants used by Defence.
Arrochar	2007 to 2009	32	B056 explained that she had seen a planned order on Horizon in October 2008 asking for £25,000 to £30,000 to be returned. She stated that she did not have this amount to return so started altering the figures at this time to agree with the Horizon figures. Throughout B056 B056 insisted that she believed this to be an administration error and had not stolen any of the money.
Kirkoswald	2008 to 2009	18	When asked why the office had been over £11,000 short on the day of the audit, again Ms A245 stated that this was due to mistakes. She claimed that she didn't always count the cash & stock properly and instead relied on the Horizon data.
Pitlochry	2009	16	When asked to explain how the shortage had occurred B057 stated that he had made an error during the summer of 2009, consisting of incorrectly entering a cash deposit into Horizon of around £31,800 rather than £3,180. He then stated that when he balanced that night Horizon showed that he was £40,000 to £45,000 short rather than the expected £28,000 to £29,000. B057 claimed that the Horizon system was ancient and was due for renewal in January 2010. He also stated that he was aware of other offices that had experienced electrical glitches causing unexplained losses. When asked to give examples of these Mr B057 stated that he would need to ask their permission before relaying any details. He has not provided any further information, (electrical fault data) despite requests.
Old Colwyn	Up to 2008	44	Audit conducted, shortage identified. Majority of loss was in the cash, Sub-postmaster believes problem with ATM. Sub-postmaster also runs Conway Road SPSO (440614) which was audited the following day, small shortage identified. Letter received from Solicitor stating suspect has been ill, but can be interviewed the week commencing 1 March to 5 March 2010 . Allegation that the Horizon data is not correct("ATM data haywire.") Unknown whether this defence will be presented in court.
Rinkfield	2008 to 2009	25	Interviewed SPMR in June 2009, admitted to false accounting, but denied theft. Solicitor now alleging that the Horizon data is incorrect.
Lazy Hill	2007 to 2009	3	Accused changed plea to not guilty. Fresh court process underway.
Alderley Edge	2008 to 2009	45	Pleaded guilty in [redacted] magistrates court. Sentenced to 3 months imprisonment suspended. Awaiting court transcripts in order to verify if the magistrate did make comments, as per press releases.
West Byfleet	2006 to 2009	75	Accused suggesting Horizon data to blame, although no specific transactions identified. Trial date set 15 March 2010
Willesden	2008 to 2009	75	Told auditors on the day of the audit that he would be short. Disputing the amount, (60K) and opposed to auditors finding of 74K, and "technical faults." Did not raise Horizon at all during the PACE interview.
Porters Avenue		72	Offender instructed a forensic accountant to analyse the data/transactions
Matfield		41	No specific transactions given relating to the Horizon database

Civil Law Cases

Current Civil cases where allegations about Horizon are an issue and where proceedings have been issued are limited to the case of B058 formerly of Sandleheath BO. We obtained judgement in default against her and were then contacted by an independent accountant who claimed to be acting pro bono for a group of aggrieved subpostmasters. He sought access to the Horizon system to examine it to challenge a long list of alleged defects with Horizon. His list was substantially culled from allegations made in the Grocer magazine. POL rejected his demands robustly and B058 collapsed consenting to a charge being issued against her property. This was sold in October to pay the debt of£28,961.

There are a number of cases on which Legal are advising on the merits of whether civil claims should be brought. These include the Alderley Edge case, B037 formerly of Odiham BO where detailed allegation about Horizon defects have been made and B059 of Alfresford BO where more general allegations have been made.

Lastly there is the threat of a class action by Shoosmith solicitors who appear to be acting for a number of aggrieved subpostmasters.

Appendix 3 – Fujitsu Report on Horizon Data Integrity

Document Title: Horizon Data Integrity
Document Reference: ARC/GEN/REP/0004
Document Type: Report (REP)
Release: N/A
Abstract: This document describes the measures that are built into Horizon to
ensure data integrity. Note that it only covers Horizon and not HNG-X (Horizon Online).
Document Status: Final Draft
Author & Dept: Gareth I Jenkins

1 Purpose

This document is submitted to Post Office for information purposes only and without prejudice. In the event that Post Office requires information in support of a legal case Fujitsu will issue a formal statement.

This document is a technical description of the measures that are built into Horizon to ensure data integrity, including a description of several failure scenarios, and descriptions as to how those measures apply in each case.

Note that this document only covers Horizon. It does not cover HNG-X (Horizon Online).

2 Horizon Data Integrity

The Horizon system is designed to store all data locally on the counter's hard disk. Once the data has been successfully stored there it is then replicated (copied) to the hard disks of any other counters in the branch (and in the case of a single counter branch to the additional external storage on the single counter). Data is also passed on from the gateway counter to the Horizon data centre using similar mechanisms.

The replication process is designed such that should the data fail to be copied immediately (for example due to a failure on the local IT network within the branch or another counter being switched off or the branch being disconnected from the data centre), then further attempts are made to replicate the data at regular intervals until it is finally copied successfully. Once the data reaches the Data Centre a further copy is taken and added into the audit trail where it is available for retrieval for up to 7 years. Data in the audit trail is "sealed" with a secure checksum that is held separately to ensure that it has not been tampered with or corrupted.

Every record that is written to the transaction log has a unique incrementing sequence number. This means it is possible to detect if any transitions records have been lost.

While a customer session is in progress, details of the transactions for that customer session are normally held in the computer's memory until the customer session (often known as the "stack") is settled. At that point all details of the transactions (including any methods of payment used) are written to the local hard disk and replicated (as described above). It should be noted that double entry bookkeeping is used when recording all financial transactions, ie for every sale of goods or services, there is a corresponding entry to cover the method of payment that has been used. When a "stack" is secured it is written in such a way that either all the data is written to the local hard disk or none of it is written. This concept of "atomic writes" is also taken into account when data is replicated to other systems (ie other counters, external storage or the data centre).

The data for a stack will have been successfully secured to the local hard disk before the screen is updated indicating that a new customer session can be started. Note that although an attempt will have been made to replicate the data to an external system at this time, there is no guarantee at this point that such replication will have been successful. For example if there is a Network Failure followed by a Terminal failure there is a slight risk that transactions in the intervening period could be lost.

All data that is written includes a "checksum" value (known as a CRC) which is checked whenever the data is read to ensure that it has not been corrupted. Any such corruptions detected on reading will result in failures being recorded in the event logs which are held on the local hard disk for a few days for immediate diagnosis and also immediately sent through to the data centre where they are held for 7 years.

Any failures to write to a hard disk (after appropriate retries) will result in the counter failing and needing to be restarted and so will be immediately visible to the user.

Whenever data is retrieved for audit enquiries a number of checks are carried out:
1. The audit files have not been tampered with (ie the Seals on the audit files are correct)
2. The individual transactions have their CRCs checked to ensure that they have not been corrupted.
3. A check is made that no records are missing. Each record generated by a counter has an incremental sequence number and a check is made that there are no gaps in the sequencing.

3 Scenarios

It should be noted that these scenarios are all to do with equipment failures and these will always be visible to Fujitsu through the event logs which are retained.

3.1 A counter fails

When a counter fails, there are two possible scenarios:
- It can be successfully restarted
- It cannot be successfully restarted, so needs to be physically replaced

In each case the Data Integrity considerations are different and so are described separately below.
Once the counter has been restarted (regardless of whether or not it has been replaced) recovery may be carried out if recoverable transactions are detected on the counter. This is also discussed below.

3.1.1 The Counter is Successfully Restarted

In this case all the data that had been secured prior to the failure is still present on the counter and so is available for use. If the User is in any doubt as to whether a transaction had been completed or not prior to the failure they can use the transaction logs to confirm one way or the other.

3.1.2 The Counter is Physically Replaced

In this case there is no data on the local hard disk of the replacement counter. However, since the data should have been replicated to other counters in the branch (or in the case of a single counter branch to the external storage – which should have been physically moved to the replacement counter), then the data should be retrieved and copied to the new counter. If for some reason the data were not available locally in the branch, then it will be copied back from the data centre. This all happens automatically as part of the counter replacement procedure.

Note that the hard disks are encrypted so there is no danger of data protection issues once the old counter has been removed (or if it is stolen).

When a counter is physically replaced, there is a possibility that not all data has been successfully replicated to another system prior to the failure. In this scenario it is essential that the user confirms what the last successful transaction on that counter was, again by using the transaction logs.

3.1.3 Transaction Recovery

Some classes of transaction generate recovery data as they go along, so as to ensure that in the event of a failure between the transaction starting and the basket being secured, there is sufficient information available to enable the transaction to be recovered. On Horizon there are two separate mechanisms to cover different classes of transaction:

- Banking Recovery
- AP Recovery

Both these mechanisms are automatically invoked during Log On, should the system detect that there has been a possible failure. These are described below.

3.1.3.1 Banking Recovery

This covers credit card and debit card transactions and e-Top-Up transactions as well as online banking transactions.

A check is carried out to see if any incomplete banking style transactions (i.e. network banking, credit / debit card or e-Top-Up) exist in the transaction logs for that counter. An incomplete transaction is one where an authorisation request has been sent to the financial institution, and there is no corresponding completion message which is normally secured as part of settlement at the end of the Customer session.

In most cases, recovery information stored in the transaction log can be used to ascertain the outcome of the transaction being recovered and a suitable completion record is then recorded at the time of recovery.

In some cases the user is prompted to confirm whether or not the transaction has completed successfully and the response from that prompt is used to generate the completion record.

3.1.3.2 AP Recovery

In the case of Automated Payments (AP), the user is asked if they wish to carry out AP recovery and they have the option of doing so immediately or leaving it until later.

If the user carries out recovery they will be asked about the last successful AP transaction (which can be seen from the branch copies of the AP receipts that are printed) and the system will then check to see if it has been completed in the system. If it has not been completed in the system, then the system will use the AP Recovery data stored in the transaction logs to ensure that all incomplete AP transactions on the counter up until the one specified by the user are completed at recovery time. To assist with this process, each AP transaction has a unique, incrementing sequence number which is printed on the receipt.

Fujitsu understand that these processes are defined in Post Office's Horizon User Guides.

3.2 A counter has a "Blue Screen of Death"

This is just a special case of a counter failure, so please see section 3.1 above.

3.3 There are package collisions on networks

The replication protocols used to copy details of transactions between counters and also between the gateway counter and the data centre ensure that the data is copied successfully.

Should packets collide on the network (or should there be any other network issues such as the IT communications link failing) then the replication protocols will ensure that the data is re-sent. Such retries will continue until the data is finally successfully transmitted.

Appendix 4 - Screen Freeze / Recovery

The HNG-X architecture allows transactions to be built up on the counter in a basket. Simplistically, the settlement of the basket is the point at which the clerk is informed that the customer transactions have been **committed to the Data Centre** and thus the signal to the clerk to **complete the exchange of goods and money with the customer**. However, some customer transactions have a more immediate effect as they happen; for instance they generate valuable artefacts or involve interactions with external systems before the point of settlement. Examples of such customer transactions are:

- On-line Banking
- Settlement with Credit / Debit Card
- E-Top ups
- DVLA Transactions
- APOP Generic Online (including Postal Orders and Moneygram)

Should such customer transactions have been included in a basket that failed to complete (eg due to system freeze, loss of connection), then some action is required to recover the customer transaction and return the overall system into a consistent state. In order to support this, recovery data is stored at the Data Centre regarding recoverable transactions to assist with the recovery process.