POL00338297

Post Office Ltd Security Performance Pack

Period 4 – 2010/11

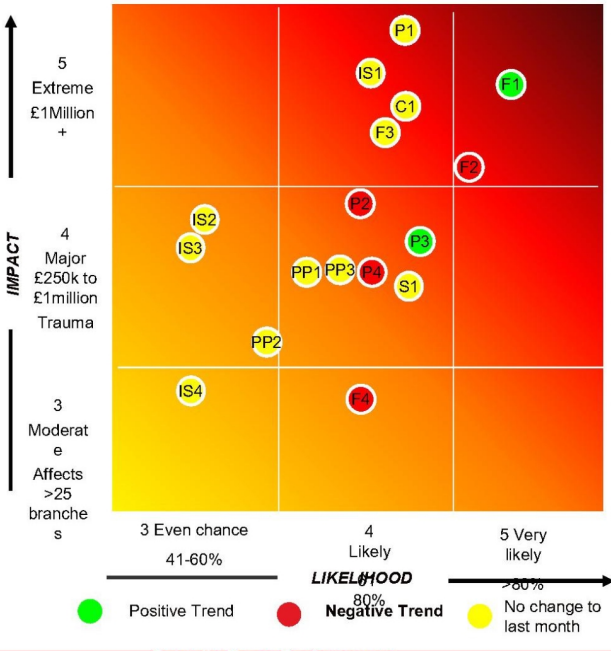
POL00338297

Contents

Risk Indicator Key	
	Positive Trend
	No Change To Last Month
	Negative Trend

POL00338297

SECURITY RISK SUMMARY



Physical Crime Primary Cash Loss Risks

Risk P1 – Slide A2 Supply Chain Cash Centre/Depot Robbery (Industry remains on high alert)

P2-A1/A3 Network Robbery (over target in period, under target year to date - full year forecast increase from £829k to £940k vs £1.052m target)

P3-A2/A3 Cash In transit Robbery (forecast decreased from £729k to £633k)

P4-A1/A4/A5 Network Burglary (forecast increased to £497 (over target) from £451k)

Physical Crime People Impacts

PP1-A1/A3 Network TIGER hostage (mainly NI risk, status due to Intelligence)

PP2-A1/A3 Northern Ireland Robbery (threat continues into new year)

PP3-A2/A3 Supply Chain Depot/Cash Centre TIGER hostage (high impact)

Fraud Risks

F1-A8 ONCH inflation of Cash In Tills (offices over target are over holding £41m)

F2-A9 Crown Office Losses including fraud (YTD £643k> target of £490k)

F3-A13/A14 False accounting of stock (Inc Savings Stamps, Scratchcards & Swindon issues)

F4-A11/12 RM Revenue Theft, Rejected and Spoilt Postage Labels (non cash impacts)

Commercial Security Cash Loss Risks

C1-A18 Telephony bad debt inc fraud (£1.7m write off to P2, full year budget £3.3m plus £2m provision, compared to £4.5m last year)

Security Cash Loss Risks (Combined Physical & Fraud)

S1-A5 ATM Crime (Rob, Burg & Fraud)

Information Security Risks – Non Cash Impacts

IS1 –A20-A23 Governance
IS2 –A20-A23 3rd Party Management
IS3 –A20-A23 Solution Design
IS4 –A20-A23 Client Management

* Where a target exists trend is based on FYF, otherwise month on month or year on year movement

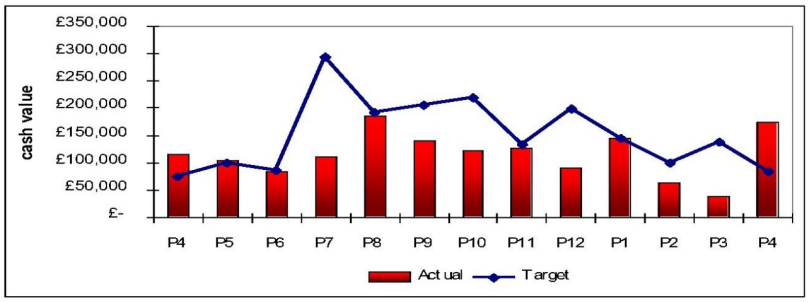
(Crime Risk: Chris Thorpe – GRO

POL00338297

A1. Post Office Branch Network Robbery & Burglary Losses

Crime Risk – P2/4 & PP2.

Crime Risk Indicator



Commentary

- The full year forecast is £1463k against a target of £1540k, which is £77k or 5% below target.
- Current period combined losses are 111% or £92k over target, £175k against £83k target.
- Year to date combined cumulative losses are 10% or £45k under target, £419k against £464k target
- Year on year comparison of current period shows 51% or £59k increase, £175k against £116k previous year
- Year on year comparison of cumulative losses shows losses of a 29% or £169k decrease, £419k against £588k previous year
- Incident numbers for the period are 3% higher than the previous year's (32 v 31) with cumulative numbers being 38% lower (85 v 137)
- Burglary losses for the period were 46% or £22.5k over target (£72k v £49k) and 120% or £39k higher than the previous year (£33k)
- Robbery losses for the period were 190% or £64k over target (£98k v £34k) and 19% or £16k higher than the previous year (£82k)
- BBA Industry trends show Met, GMP & W Yorkshire (Robbery) and Met & W Midlands (Burglary) police force areas are suffering from the highest volumes of crime
- 5 Line cuts occurred this month, 2 BOI sites TS6 & SW4, 1 Hanco TS29, WV13 & CV33 (no ATM on site)

Mitigating actions, update and status

- Task Force Vehicles continue to provide health checks and reassurance visits in the North West & W.Yorks, although their main focus remains covering cash deliveries
- Sussex Police are still continuing their rounds on Adopt a Post Office raising the profile of partnership working
- The Security Team are currently engaging with the Met Police in relation to an increase in gun enabled crime within the area

POL Security definitions of Robbery & Burglary differ from the UK criminal legal definition for analysis/statistical reasons. Robbery is defined as including a threat or actual violence; this includes aborted and apprehended attempts where assailants were prepared to rob. Burglary is defined as including any attempt on a premise containing a Post Office (includes broken locks, alarms, lines cut etc).

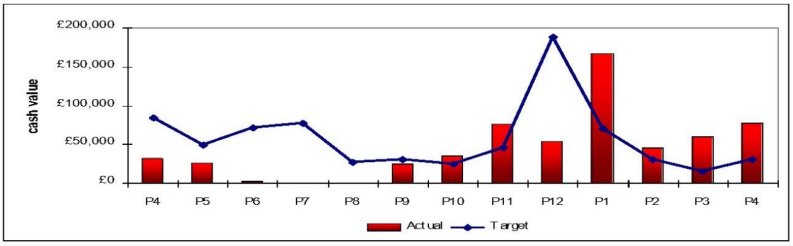
POL00338297

A2. Supply Chain Robbery Losses

[Please note new Supply Chain Target]

Crime Risk – P3.

Crime Risk Indicator ⇩



Commentary

- The full year forecast is £633k against a target of £300k which is £333k or 111% above target. *[This reflects Supply Chains Target]*
- Year to date cumulative losses year are 142% or £206k over target, £351k against £145k target. *[This reflects Supply Chains Target]*
- Year on year comparison of current period shows 140% or £45k increase, £77k against £32k previous year
- Year on year comparisons of cumulative losses shows a 77% or £152k increase, £351k against £199k previous year
- Incident numbers are 80% higher than at the same level year on year (9v5) with cumulative numbers 14% lower (24v28)
- Ytd 66% of Supply Chain losses occurred within the London area depots covering the Metropolitan area accounting for 46% of the volume of crime
- Ytd 8% of Supply Chain losses occurred from the Manchester depot, accounting for 17% of PO Supply Chain volume of crime
- Based on industry data the Metropolitan police force had 28% of industry losses with 49% of the volume of crime (Jan to Jun)
- For Jan to June, GMP had 17% of industry losses and 11% of the volume of crime and Merseyside had 2% of the losses and 2% of the volume
- Early Indications for industry incident numbers for July are down on June (68 June v 52 July), with the Met, West Yorks and West Mids showing the highest levels

Mitigating actions, update and status

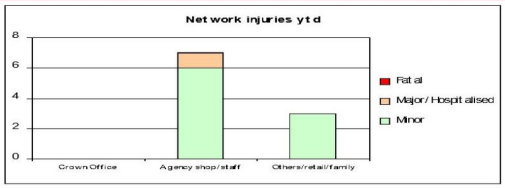
- Post Office funded Task Force vehicles have been deployed within the Metropolitan, West Yorkshire, GMP, West Mids & Merseyside police areas
- Police operations ("Vanguard" in the Met force area; "Vanguard" in Manchester, "Guardian" in Merseyside & armed response in W. Mids) were deployed in the period
- Police visited Dartford & Midway depots to increase awareness and engagement.
- West Yorkshrie Police continued to support CViT services in the Leeds area
- ~~Security advisors are working with depots to implement local fixes identified as part of Operation Ingress 2 project~~

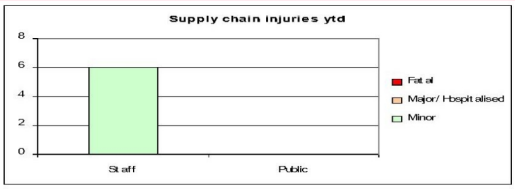
POL Security definitions of Robbery & Burglary differ from the UK criminal legal definition for analysis/statistical reasons. Robbery is defined as including a threat or actual violence; this includes aborted and apprehended attempts where assailants were prepared to rob. Burglary is defined as including any attempt on a premise containing a Post Office (includes broken locks, alarms, lines cut etc).

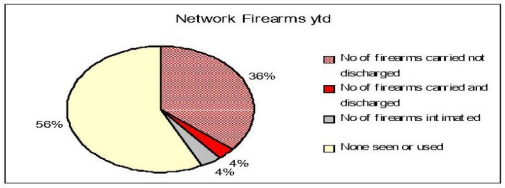
POL00338297

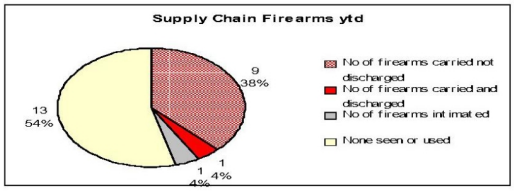
A3. Supply Chain and Network – Firearms & Injury

Crime Risk – P2/3.









Commentary

Supply Chain

- 3 of 9 Supply Chain incidents for the period were carried out with firearms present or intimated, bringing the cumulative total to 11 of 24 with firearms present, compared to 0 incidents for the period and 6 of 28 cumulative for the previous yr to date [2009/10]
- 5 injuries were reported for Supply Chain incidents during the period, bringing the cumulative total to 6 (crew) minor injury, compared to 3 injuries for the period and 11 (10 crew & 1 public – all minor) cumulative for the year to date [2009/10]

Network

- 8 of 13 Network incidents for the period were reported where firearms were present or intimated, bringing the cumulative total to 20 of 40 with firearms, compared to 5 of 9 for the period and 22 of 50 cumulative for the previous yr to date [2009/10]
- 4 injuries (3 minor & 1 major & 2 other minor) were reported for Network incidents during the period, yr to date total of 10 (7 agents & 3 other), compared with 3 (minor, 1 agency & 2 other) for the period and 8 cumulative for the year to date (6 agents & 2 other) [2009/10].

Mitigating actions. Update and status

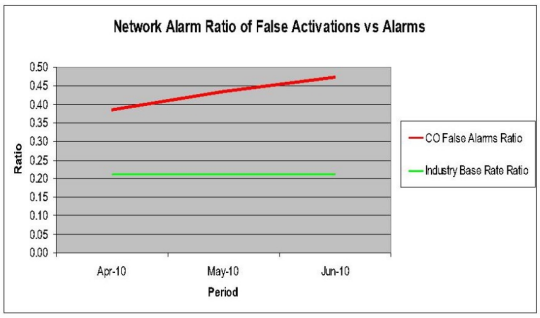
- The Security Team are currently engaging with the Met Police in relation to an increase in gun enabled crime within the area
- Annual review of risk for Supply Chain to determine business policy on the use of body armour.

POL00338297

A4. Crown Office False Alarms

Crime Risk – P4.

Crime Risk Indicator



Commentary

- The Crown Network branches have experienced a total of 2538 False Alarms yr to date from 375 branches, with 839 occurring during period 2.
- Estimated Cost of Group 4 Keyholder Callouts to false alarms yr to date is £33.3k, with £11.3k costs during period 2.
- There are currently 20 CO Branches that will require the system to be upgraded at a cost of c£10k per system to regain police response, a business case has been submitted for this.
- Opportunity identified to reduce policed FA numbers - numbers had been high due to system reporting error where some FA's were counted as double, this has now been rectified, overall numbers reduced and new targets set based on corrected historical data.
- The number of Policed False Alarms during period 3 was **17**, cumulative yr to date **44**, compared to **41** in the same period last yr and a cumulative total of **90** yr to date last yr. This is currently **22 ahead of target, resulting in a forecast yr end figure of 176.**
- The target to reduce Policed False Alarms is 20% this year to 265, the yr end outturn was 331 (2009-10).
- The industry Policed False alarm ratio is 1 : 0.21, at period 3 (yr to date and annualised) the Crown Office ratio is 1 : 0.47, [approx 2 times higher].

Mitigating Actions

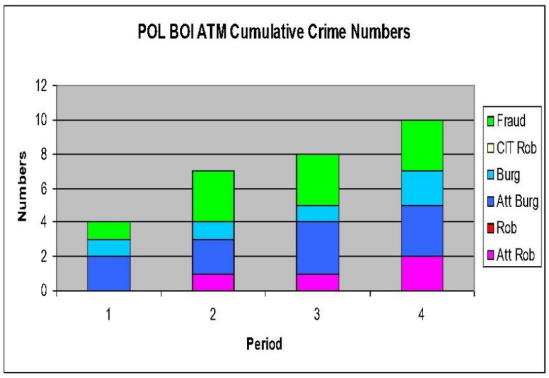
- Equipment team contacting branches post key holder call out to discuss each issue.
- Industry comparison data highlighting that CO performance is poor in comparison.
- Phone calls made to branches post policed alarm to establish reason and aid branch earning - list of do's and don'ts emailed to branch
- Phone calls made to branches with the highest number of non-policed false alarms [top 10] – to reduce call out costs and educate the branches on the issues.
- Crown focus article issued as a reminder to ensure alarms are set when leaving the branch, reduction in call out costs
- ~~Generic comms to be issued at the end of June to branches with high levels of G4 keyholder call outs to reduce costs~~

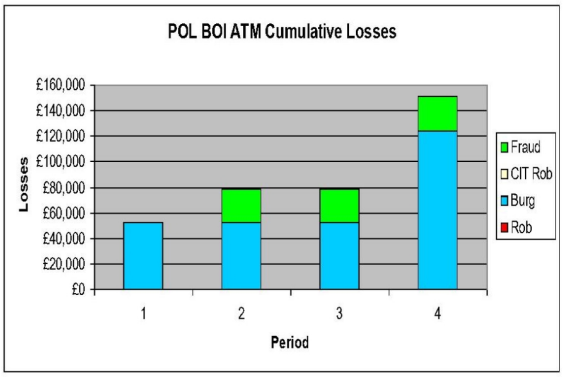
POL00338297

A5. Automated Teller Machine (ATM) Crime

Crime Risk – S1

Crime Risk Indicator ⟺





Commentary

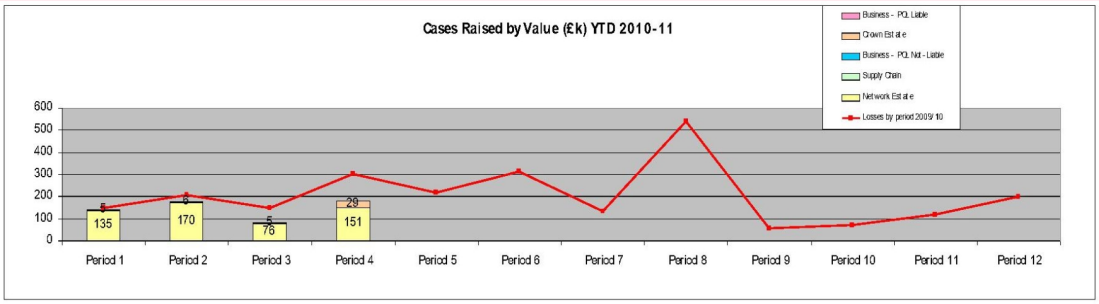
- 2 ATM related incidents occurred in period 4, (1 att robb – M18 & 1 burg – CH2), compared to 2 for period 4 last year [09-10].
- Total crime losses yr to date amount to £150.6K from 10 ATM related incidents, compared to £144.7k from 5 incidents last yr.
  - 10-11 ~ 2 burglaries - £124.4k, 3 attempted burglaries, 2 attempted robbery, 3 Fraud - £26.1k
  - 09-10 ~ 2 burglaries - £79.7k, 2 attempted burglaries, 1 Fraud - £65k
- BBA Industry trends show Avon & Somerset, W Yorkshire & Cheshire are suffering from the highest level of ATM crime

Mitigating actions, update and status

•Security, Network Support & the ATM Service Team are reviewing branches that regularly declare in excess of their maximum ATM cash limits.
•Arrangements have been made to deploy temporary fogging kits to branches in the Chester postcode area

POL00338297

A6. Casework - losses by type



Commentary

- Casework losses year to date amounts to £578k in 71 cases, an average loss of £8k
  - [compared to £804k in 67 cases for 2009/10, same period, with an average loss of £12k].
- Audit deficiencies year to date amount to £355k, 61.4% of all casework raised (value).
  - [compared to £652k, 85% of all cases raised for 2009/10 (value), same period].
- An average audit loss of £14.2k per case in 25 cases raised year to date
  - [compared to an average of £15.9k per case in 41 for 2009/10, same period].

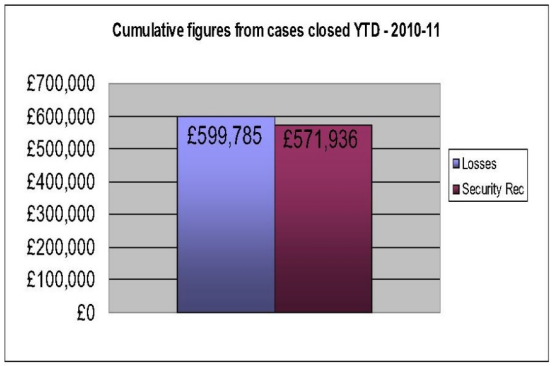
Highest Loss cases raised in period 4 – 2010/11

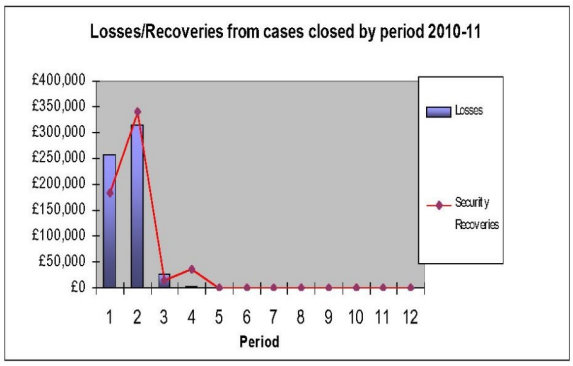
Case Ref No	Date Raised	Main Case Type	Enquiry Type	Office / Location	Branch code	Initial Loss reported	Current Loss
POLTD/1011/0059	19/07/2010	Theft	Cash Loss	BLACKWATER	083900	£58,000.00	£58,000.00
POLTD/1011/0061	26/07/2010	HNGX	Cash Loss	FORD	219420	£36,191.51	£36,191.51

POL00338297

A7. Asset Recovery Against Fraud

Crime Risk Indicator ⬆





Commentary

- From 53 cases closed, year to date £571.9k has been recovered against identified losses in those cases of £599.8k [compared to £819k against £800k last yr].
- The year to date figure for recoveries is 95.4% [compared to 102.4% last yr for the same period].

Mitigating actions, update and status

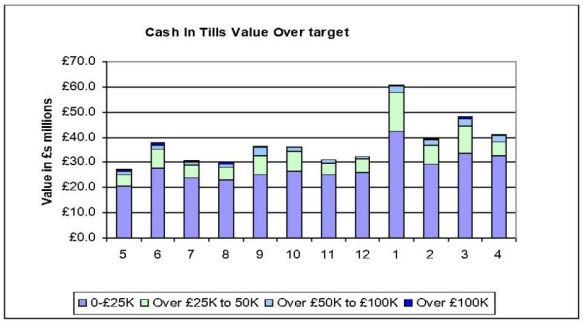
- Dave Posnett joined the FIU as a Financial Investigator on the July 5th and has started his FI training programme. Dave has also commenced working on his own financial investigation cases and now has access to the NPIA computerised support system.
- Successes- POLTD/0910/0063, Confiscation hearing, order made for the repayment of £18.7k plus interest of £1.9k within 6 months. Will be 100% recovery, restrained assets in place to fulfil the Court order.
- POLTD0910/0014, In order to avoid going into confiscation, the defendant requested a variation to the Restraint Order. The Order was accordingly varied by the FIU and as a result the full amount of the loss of £74.8k was recovered without recourse to a confiscation hearing.

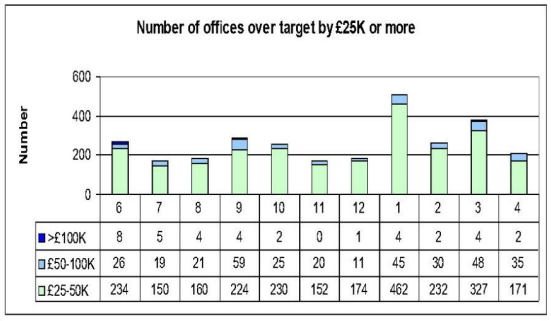
POL00338297

A8. Cash In Tills Over Night Cash Holdings (ONCH)

Crime Risk – F1.

Crime Risk Indicator





	6	7	8	9	10	11	12	1	2	3	4
>£100K	8	5	4	4	2	0	1	4	2	4	2
£50-100K	26	19	21	59	25	20	11	45	30	48	35
£25-50K	234	150	160	224	230	152	174	462	232	327	171

Commentary

- At Period 4 there were **5350** offices over target, down from **6013** in Period 3.
- The number of offices £25K or more over target was **208**, down from **379** in Period 3.
- Overall value at over target offices is **£40.9m**, down from **£48.1m** in Period 3.
- Overall Retail Cash In Tills holdings were over target by -**£5.57m**, down from +**£3.88** in Period 3.

Mitigating actions, update and status

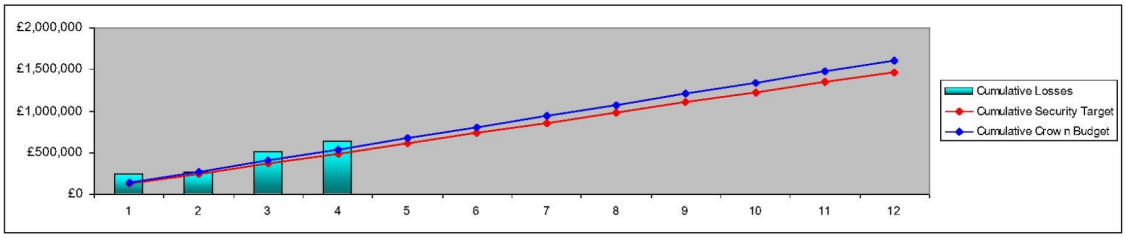
- Security and CRM Team Bristol met to agree and discuss proposed program activity following Horizon Online migration, sometime in October 2010.
- Horizon Online - migrations and associated cash verifications remain suspended until problems are rectified. Stakeholders have been identified and agreed in respect of proposed weekly fraud conference calls once full migration is rolled out. The Sharepoint site that captures all migrating branches and relevant data has now been communicated to all stakeholders.
- Security are aiming to implement monthly BAU intervention activities at branches where ONCH concerns are evident. In conjunction with Cash Management, a number data streams are being evaluated to ascertain the most appropriate data for targeting purposes.

POL00338297

A9. Crown Office Loss Initiative

Crime Risk – F2.

Crime Risk Indicator



Commentary

- The budget for Crown Office losses in 2010/2011 is **£1.61m**, equating to **£134k** per Period. The Security Team objective aims to support this and also aspire to a **10%** reduction against last years losses, representing a target of **£1.47m** of losses at year end. This equates to **£122.5k** of losses per Period.
- Data used for this programme reflects the actual net losses and gains posted to the accounts by Crown Offices. It does not factor in adjustments for known Transaction Corrections or incorrect/omitted postings, both of which should result in compensating errors when and where identified.
- The losses in Finance Period 4 totalled **£138.7k.** Cumulative losses stand at **£643k** year to date, against a year to date target of **£490k.** Losses in Period 4 were slightly in breach of both Crown budget and Security target and are cumulatively **23.8%** in breach of ytd target.
- **£122k** of losses this Period affect only 6 Crowns. The majority (**£120k**) are due to known errors or mis-keys where TC's will be posted during period 05.

Mitigating actions, update and status

- Regional Support Advisors continue to target the worst 80 performing branches each month. A pro-forma is completed by Branch Managers, to demonstrate Losses & Gains policy adherence, along with compliance to Security, Cash Declaration and Transaction Correction procedures.
- A matrix of Security activities associated with Crown loss reduction has been submitted to the Head Of Crown Efficiency. A meeting held with the Crown Team has identified next steps around developing root cause analysis, a review of the Security toolkit and comms to support intervention activity in September/October.
- Root cause analysis of losses by Security is now complete. This has identified the ratio of losses v Transaction Corrections and the most prevalent Transaction Corrections in terms of volumes and values across the Crown estate and per branch.

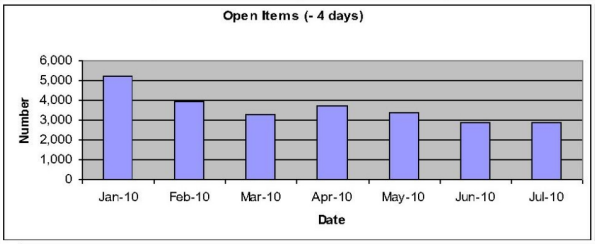
POL00338297

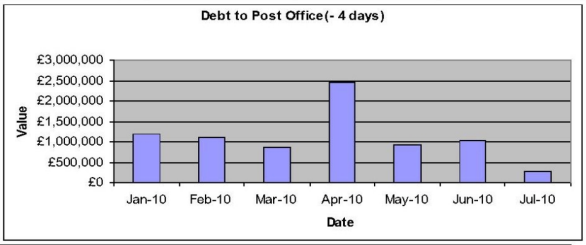
A10. Cheques/Open Items

Crime Risk – F.

Crime Risk Indicator

15th of Month	Jan-10	Feb-10	Mar-10	Apr-10	May-10	Jun-10	Jul-10
Open Items (- 4 days)	5,221	3,925	3,292	3,716	3,385	2,914	2,907
	Jan-10	Feb-10	Mar-10	Apr-10	May-10	Jun-10	Jul-10
Balance(- 4 days)	£1,197,803	£1,097,486	£865,642	£2,460,928	£912,011	£1,018,682	£281,741
	Jan-10	Feb-10	Mar-10	Apr-10	May-10	Jun-10	Jul-10
Number of offices	1,704	1,448	1,186	1,317	1,213	1,108	1,000





Commentary

- The net balance deficit to Post Office Limited (allowing 4 days for receipt) in cheque discrepancies was £281k at 15th July with 5 offices (down from 11 last month) showing a debt of £25k or more this month.
- There were 26 offices with 10 or more open items (up from 16 last month), but only 2 offices with more than 20 open items.
- No items over 4 months are currently unresolved.
- The average value of each open item has fallen from £350 last month to £97 this month.
- The average balance of open items per office has also fallen from £919 last month to £282 this month.

Mitigating Actions, update and status

- P&BA are continuing to contact offices on a daily basis to target those showing cheques at site balances and to resolve open item issues.
- The security team have been working with P&BA to develop a monthly cheque risk scoring for all offices to feed into the branch profile, which is currently being redesigned.

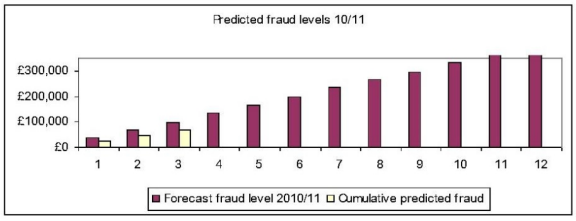
POL00338297

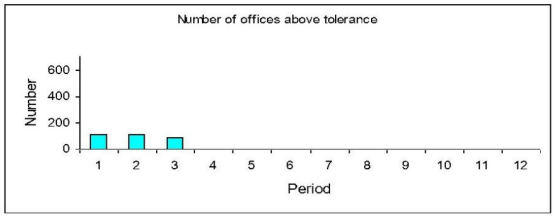
A11. Rejected Postage Labels

Crime Risk – F4

Crime Risk Indicator

Period	1	2	3	4	5	6	7	8	9	10	11	12
Predicted fraud level 2010/11	£25,619	£20,019	£19,796									
Cumulative predicted fraud 2010 / 2011	£25,619	£45,638	£65,434									
Cumulative forecast fraud 2010 / 2011	£37,785	£68,013	£98,241	£136,026	£166,254	£196,482	£234,267	£264,495	£294,723	£332,508	£362,736	£392,964
Number of offices above tolerance	109	111	91									





Commentary

- Period 3 figures have now been revised to remove offices reporting printer problems and offices migrating to HOL.
- These offices have only been removed if they have not previously appeared above tolerance in April and May 2010.
- The data for July is currently being analysed using the same method to ensure that the predicted fraud figures are adjusted accordingly.

Mitigating Actions, update and status

- As offices are migrating it has become clear that the value of rejected labels are increasing. Investigation into June's figures showed that out of 95 offices included in the predicted fraud figure, 91 had migrated and had not showed as above tolerance in the previous 2 months prior to migration.
- The current labels being used are causing problems with the printers with 3331 calls reporting faults in July 2010 received, compared to 1497 in July 2009. A new label has been developed and is due out for testing imminently.

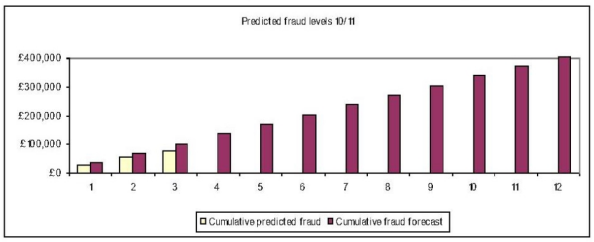
POL00338297

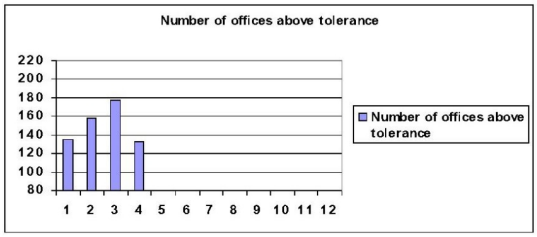
A12. Spoilt Postage Labels

Crime Risk – F4

Crime Risk Indicator

Period	1	2	3	4	5	6	7	8	9	10	11	12
Predicted fraud level 2010/11	£27,502	£27,478	£23,010									
Cumulative predicted fraud 2010/2011	£27,502	£54,980	£77,990									
Cumulative fraud forecast 2010 / 2011	£38,683	£69,629	£100,575	£139,258	£170,204	£201,150	£239,833	£270,779	£301,725	£340,408	£371,354	£402,300
Number of offices above tolerance	135	158	133									





Commentary

- Period 3 figures have now been revised to remove offices reporting printer problems and offices migrating to HOL.
- These offices have only been removed if they have not previously appeared above tolerance in April and May 2010.
- The data for July is currently being analysed using the same method to ensure that the predicted fraud figures are adjusted accordingly.

Mitigating Actions, update and status

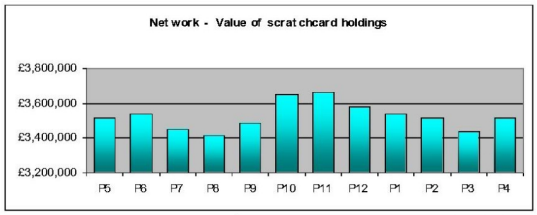
- As offices are migrating it has become clear that there can be teething problems with spoilt postage. Investigation into June's figures showed that out of 32 offices included in the predicted fraud figure, 10 had migrated and had not showed as above tolerance in the previous 2 months prior to migration.
- The current labels being used are causing problems with the printers with 3331 calls reporting faults in July 2010 received, compared to 1497 in July 2009. A new label has been developed and is due out for testing imminently.

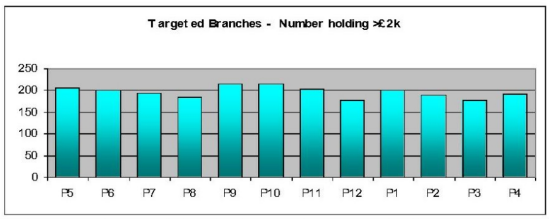
POL00338297

A13. Lottery Scratchcards

Crime Risk – F3

Crime Risk Indicator





	P5	P6	P7	P8	P9	P10	P11	P12	P1	P2	P3	P4
Network - Branches holding scratchcards	3368	3363	3350	3320	3320	3454	3457	3462	3431	3427	3419	3,432
Network - Value of scratchcard holdings	£3,517,315	£3,538,974	£3,448,998	£3,413,788	£3,483,394	£3,652,376	£3,664,154	£3,581,091	£3,540,380	£3,514,844	£3,438,415	£3,516,790
Network - Average holdings per branch	£1,044	£1,052	£1,029	£1,028	£1,049	£1,057	£1,059	£1,034	£1,031	£1,025	£1,005	£1,024
Targeted Branches - Number holding >£2k	206	202	195	185	216	215	203	178	201	190	177	192
Targeted Branches - Value holding >£2k	£627,889	£592,475	£567,236	£528,521	£612,394	£639,989	£557,203	£504,658	£526,001	£517,322	£485,480	£529,193
Targeted Branches - Average holdings >£2k	£3,048	£2,933	£2,909	£2,856	£2,835	£2,976	£2,744	£2,835	£2,617	£2,722	£2,742	£2,756

Commentary

- Across the Network: There are **3432** branches holding **£3.5m** of scratchcards, with an average value of **£1k** per branch.
- Targeted Branches holding >£2k: There are **192** branches holding **£529k** of scratchcards, with an average value of **£2.7k** per branch.
- Key measurement: Branches in breach of £2k target increased in P4. The **192** branches represent **1** Crown, **37** Multiples and **154** Independents.

Mitigating actions, update and status

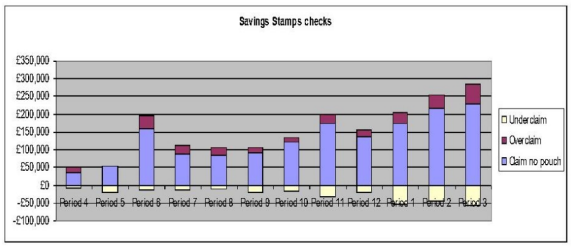
- The Feasibility report concerning the PING project has been circulated. Subject to HNGX delays and phased removal of scratchcard games, the estimated completion of full PING migration will be February 2011. This will facilitate better monitoring/controls in respect of scratchcard movements.
- 11 interventions have been requested by Security year to date, based on the level of scratchcard holdings and trends. These have identified £46k of losses, of which £35k relates directly to scratchcard concerns. BAU Interventions have now been postponed until HNGX migrations are complete.
- Security have been supplied with dispenser data for all branches and are currently working on overlaying this data so that more accurate targets can be applied. There are some alignment issues requiring resolution before data for period 4 can be re-evaluated.

POL00338297

A14. Savings Stamps

Crime Risk – F3.

Crime Risk Indicator



	Crown Period 1		Multiple Period 1		Crown Period 2		Multiple Period 2	
	Value	Branches	Value	Branches	Value	Branches	Value	Branches
Claim no pouch	£0.00	0	£1,625.00	4	£0.00	0	£270.00	1
Over claim	£0.00	0	£140.00	2	£0.00	0	£365.00	2
Under claim	£0.00	0	-£5,405.00	4	£0.00	0	-£310.00	1
Net	£0.00	0	-£3,640.00	10	£0.00	0	£325.00	4

Number of offices	Period 12	Period 1	Period 2	Period 3
Total Checks	2899	2935	2851	3029
Claim no pouch	265	337	346	352
Over claim	109	118	123	182
Under claim	79	159	132	161
Total discrepancies	453	614	601	695

Value of discrepancies	Period 12	Period 1	Period 2	Period 3
Claim no pouch	£136,885	£172,780	£216,100	£228,825
Over claim	£19,450	£32,280	£37,110	£57,505
Under claim	-£19,050	-£53,385	-£43,405	-£55,425
Net	£137,285	£151,675	£209,805	£230,905

•Mitigating Actions. Update and status

- Robust processes are now in place at Swindon to perform a 100% check on all returned unsold POSS.
- Credence report finalised to track deposits onto new automated budget card.
- 15 overclaims totalling £10.4k and 8 underclaims totalling £4.2k discovered to date in returned POSS checked at Swindon.
- Just over £2.5 million in unsold POSS left out in the network.
- Process allowing P&BA to pick up the discrepancies posted by Swindon has been checked and appears to be robust.

POL00338297

A.15 Commercial Security

Key:

Green	Low risk/no concern
Amber	Medium risk/concern
Red	High risk/concern

POST OFFICE®

Products	Current Status
	Financial Services
G20 Transcash Fraud	**Issue :** Phase 1: Transcash G20's are manual deposit slips that are mainly used for bill payments or making cash deposits into Business accounts & for making donations to a Freepay account. The fraudsters are using G20's as deposits and providing a cheque as a means of payment. They clear the funds before the cheques are bounced. Phase 2: There are also pre printed G20 slips that are issued by businesses, payment may only be paid by cheque if the words "cheque acceptable" are printed on the form. The fraudsters are producing their own pre printed paying in slips and although the account number entered onto the form does not exist, they have somehow managed to place an account number into the code line details on the bottom of the paying slip. This fraud started in April and the total known level of fraud was £1,008,000. **Action :** Phase 1: We have already stopped the G20 Transcash fraud and we have measures in place to stop this kind of fraud occurring again. Phase2: There is still a problem around the pre printed format. Although this fraud is temporarily contained we cannot guarantee that it will stop permanently. Therefore, the Security team are having number of meetings with various stakeholders including the fraud team at A&L to find a long term solution and also to establish the links between the two fraud teams. Security and product teams met A&L to explore the long term solutions that would be acceptable to both parties. After implementing fraud measures at both A&L and POL systems, the level of POL liability is £147k. No further fraudulent activity to report since 14/06/10. Lessons Learned conference call has been arranged by Security for 6th of August to have a SWOT analysis on this recent event and agree on the future communications and activities to better manage an event similar to this one in future. Security will be meeting the Horizon Online team to find and implement a system driven security measure to stop this kind of fraud going forward.

POL00338297

A.16 Commercial Security

Key:

Green	Low risk/no concern
Amber	Medium risk/concern
Red	High risk/concern

POST OFFICE®

Products	Current Status
Financial Services	
PIN PED Replacement Project pre ITT	**Issue :** The Post Office Pin Entry Device (PED) currently in use is no longer seen as compliant by the payments industry. The industry target set for replacing pre Visa PED Standard devices is July 2010. As a result the Post Office PED estate is out of step with the industry in terms of standards compliance. **Action :** Security is now working with the PIN PEDs Replacement Project Pre-ITT Board to capture security requirements for the ITT.
Travel Money Card (TMC) New Generation Project	**Issue :** The current contract for the provision of the Post Office (PO) TMC card programme comes to an end in May 2011, when all aspects of the card service will end. As a strategic product in the PO travel money portfolio, this Travel Money Card Next Generation Project is to identify a replacement to the existing card programme. **Action :** Security is working with the product and the project team on the Security Risk Review and also on the required security and fraud prevention measures.
CAP Gemini Fraud Management System	**Issue :** In order to bring the group EBusiness solutions and requirements together the RMG has made an agreement with CAP Gemini, who is expert in fraud management. **Action :** Security is working with RMG and Experian to define the required security and real time fraud prevention measures on group products through a number of fraud management workshops run by Cap Gemini.

POL00338297

A.17 Commercial Security

Key:

Green	Low risk/no concern
Amber	Medium risk/concern
Red	High risk/concern

POST OFFICE®

Products	Current Status
Financial Services	
Personal Cheque Encashment Fraud	**Issue:** Fraudsters are currently targeting our offices in an attempt to cash high value A&L, Clydesdale Bank and Bank of Ireland personal cheques. Branches have been receiving telephone calls from someone claiming to be from one of our partner banks requesting that the branch carries out an emergency cheque encashment. The fraudster then provides the branch with account and cheque details along with a telephone number. The fraudster then ask for a call back to verify that the request is genuine. The calls are not genuine as we have no emergency cheque encashment arrangements with any of our partner banks. **Action:** Security and product teams issued an MBS and an Operational Focus article to re-iterate the problem to the network. Grapevine SMS messages are also sent to the affected geographical areas. Security is working with A&L, BOI, Clydesdale, SOCA, Grapevine and POL product teams to measure the actual problem and find a solution to stop this fraud occurring. Security is liaising with the Horizon Online team to find a system driven measure to stop permanently this kind of fraud happening in future.
Bureau Swipe and Signature Fraud	**Issue :** Chip & Pin drastically cut cardholder present fraud in the UK, however, fraud has migrated to cards which are not issued with chip and pin. This is because the technology behind those cards is simple and allow cards to be easily cloned and used without the owner's knowledge. POL Bureau products have been targeted by this type of fraud and YTD (Year to Date) fraud losses are £125k. **Action :** Security and RBS fraud Management have decided to issue an MBS advising Code 10, for authorisation, for Swipe and Signature Cards to stop fraud, RBS states this process is currently successful with no genuine customers being stranded so far.

POL00338297

A18. Commercial Security – risks and issues

Products	Current Status
Government Services, Mails & Telephony	
Post Office Card Account	**Issue:** The risk of internal fraud by clerks or Subpostmasters targeting vulnerable customers affecting Post Office Ltd and POCa branding **Action:** In order to proactively identify this before the customer complains, analysis of duplicate transactions has been produced to input to the Network Branch Profile (for audit activity) and testing of suspicious profiles for piloting branch interventions, with the Network. JP Morgan are developing the key filter identified and exploring others to identify potential fraud in real time at source. Recent activity has highlighted the non-conformance of branches to the rules pertaining to holding of POCa cards and/or PINs for customers, with some fraud arising from this and how to contain this is being raised with the Network Teams.
DVLA	**Issue:** The risk of fraud (particularly internal) negatively affects the DVLA relationship and contract. **Action:** Ongoing fraud liaison meetings are held with the DVLA held to discuss their current concerns. Analysis, specific branch intervention and the wider 'Top Tips' communications programme has shown a large reduction in manual transactions in the post invention monitoring. Current concerns are the volume of 'able to disable', change of taxation class transactions that could be an opportunity to misappropriate tax revenue due to the DVLA and analysis and data sharing is being developed to inform a programme.
Mails Integrity	**Issue:** Non-compliant offices in the network. **Action:** Compliance checks as part of HNGX roll out continued through July with 5621 completed (source: Sharepoint) of which 5370 were compliant and 251 non-compliant. The Equipment Team are monitoring the non-compliant numbers and sending to the Compliance Team for process adherence. Installations of equipment at existing non-compliant branches began in January with 67 installations completed and 37 non compliant remain being managed similar to above.
Telephone Debt	**Issue:** Telephony bad debt out turned at £4.5m last year and at P2 this year £1.7m was written off. The full year budget for write off is £3.3m with an additional £2m provision. **Action:** Although debt in relation to income is relatively low and third party management of the debt is in place, in line with Industry practice and debt levels, the absolute value of debt is [illegible] losses project.

POL00338297

A19. Commercial Security – risks and issues

Government Services, Mails & Telephony

AEI	**Issue:** The business analysts team require fraud assurance around contract bid for new front line service for IPS. Also as the roll out progresses some installations are being queried as to the effect on Physical Security. **Action:** The bid process is underway and the Security Team will continue to provide advice through the delivery process. Liaison with the project team is to be undertaken to establish a way forward with providing assurance that installations do not affect Physical Security.
SMoTS	**Issue:** The business is developing SMoTS (simple money transmission service) to provide the service for the replacement of DWP cashcheques. Part of the contract tender process requires Fraud Assurance and policies to be provided. Security have also been asked to assess the viability of using Paystation as a supplement to out of hours encashments. **Action:** Whilst DWP assess the tender bid during the coming months Security will support the project with necessary expertise and guidance.
Business Point Pilot	**Issue:** New mails drop off service for volume transaction customers who pay a premium to avoid queuing in Post Office Branches **Action:** The product is moving towards trial with some issues addressed and security is working with the project manager to address other outstanding issues.
POL Retail ITT	**Issue:** Procurement of a new supplier for POL Retail is underway with a revised specification from current services. **Action:** Security met with procurement to understand the new business model and tender. Security are involved in security requirements for the overall procurement process as necessary. The new business model addresses some key areas of security and loss control.

POL00338297

A20. Information Security

Key:

Green	Mitigating actions in place, works going to plan
Amber	Mitigating actions in place, still some concerns
Red	No mitigating actions in place or slippage in plans

POST OFFICE®

Dimension	Current Status
Mails & Retail	
Overall	Support is being provided for a number of projects in support of the provision of Mails and Retail Services
Horizon Online	**Risk:** Failure to manage the ongoing security of the service could result in breaches to the system, lack of clarity on the overall security posture and failure of legal and regulatory requirements. **Issue:** The change to the service and contractual position with the migration to HNG-X provides opportunities to enhance the management of Information Security for the service, but also a risk that some existing good practice mat be lost. Engagement with Service Delivery is not yet fully completed and some work needs to be done on the Service Schedules to ensure ISec requirements are on board and being monitored. **Action:** Work with Fujitsu on their ISO27001 certification has resulted in the completion of a successful audit and significant improvements in the management and understanding of risk. Further work with Fujitsu and Service Delivery on reporting and monitoring is underway to improve and enhance the management of Fujitsu as a provider of the security services.
Payment Card	**Risk:** The auditors may not be satisfied that the evidence presented to them is sufficient to demonstrate adherence with the standard. **Issue:** The audit is not yet complete and there remains the possibility that the auditor may find some areas where controls are not fully met. Gaps may exist in the existing service schedules with Fujitsu such that additional commercial discussions may be required to ensure the requirements are met. **Action**: A analysis of the gaps between the existing service and that required to satisfy the PCI requirements has been conducted and only one specific area does not appear to be fully covered. A PCI specific penetration test is due to be conducted to meet the auditor's requirements and the provision of compensating controls and evidence of compliance is being prepared.

POL00338297

A21. Information Security

Dimension	Current Status
	Government Services
Overall	Resource is being provided in support of existing and new initiatives for Government Services where progress, generally, has been good.
AEI	**Risk:** Failure to maintain the necessary accreditation and assurance level through periods of system and product change. **Issue:** Ongoing requirements from clients for accreditation of changes to the system components results in the need for repeated re-accreditation activities which are time and resource intensive. Ongoing management of these client expectations requires frequent engagement and resource especially as that which was dedicated to the project is now no longer available. **Action:** The latest accreditation document set has been submitted and is expected to be "passed". The security review boards are scheduled with clients and are being used as a forum for the exploration of any outstanding issues and provision of client assurance.
POca	**Risk:** Key components may not met the necessary security requirements. **Issue:** A risk has been raised around the lack of control in counter operating procedures which has been flagged on numerous previous occasions, meeting resistance from product owners due to the implications for transaction times. A component of the HNG-X infrastructure is planned to be used as part of the fulfilment process and assurance of the suitability for this purpose needs to be obtained. **Action:** The risks surrounding the operational controls continue to be monitored and assessed against the other system controls and opportunities. A penetration test of the HNG-X component is being undertaken as is a further review of the design documentation.

POL00338297

A22. Information Security

Dimension	Current Status
	Financial Services
Overall	Engagement in the change of existing products and development of new ones continues to improve and recent activities have enhanced the progress through the "Gating" process.
Banking	**Risk:** Changes to banking systems in support of non-relevant PCI requirements may result in failures of interfaces. **Issue:** Those interfaces which may be changed are being reconfigured, although there remain legacy interfaces where any change would result in the failure of communication. **Action:** The changes to the interfaces have been assessed for the legacy systems and the changes are being addressed by the client.
BOI/POFTS	**Risk:** Governance from BOI may not be appropriate to address regulatory and commercial concerns. **Issue:** There is a lack of clarity around responsibility in BOI/POFTS for information security. The Bank structure is not as clear as in POL and this continues to result in issues with gathering the right group for a forum. **Action:** Escalation through the appropriate forums and via the collaboration work with Service Delivery continues.

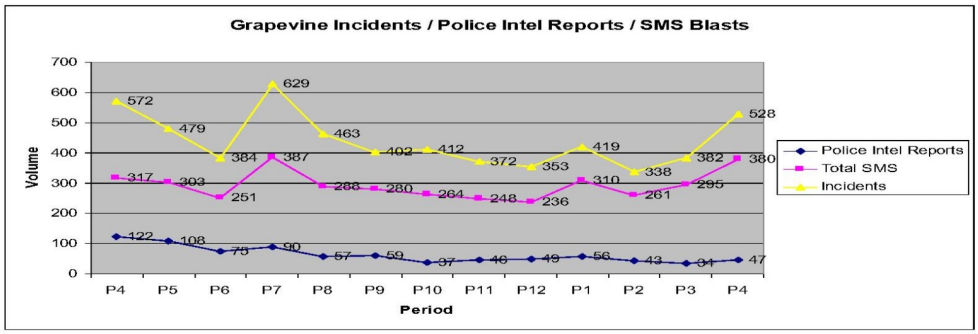
POL00338297

A23. Information Security

Dimension	Current Status
Telephony	
Overall	Direct involvement in this area is currently directed towards the Homephone/broadband product, although many other areas impact here as well.
Broadband	**Risk:** Our suppliers outsource and offshore to Third parties without the necessary assurance that Security requirements can be maintained. **Issue:** Offshoring and outsourcing activity is continuing with pressure being brought to bear by BT without the necessary support and involvement of their own security people. **Action:** Collaboration with the product owner, legal and BT security is resulting in improvements to the visibility of controls being deployed and under the control of the contract.
Programmes & Infrastructure	
Overall	Programmes to look at the use of administrator accounts, vulnerabilities on the infrastructure and training and awareness are currently underway. Engagement with POL project to replace Lotus Notes.
RMG	**Risk:** RMG fail to provide essential information security improvements with a corresponding impact of POL's ability to do business accordingly. **Issue:** Some RMG projects continue to reach quite advanced stages without involvement from POL, despite the business being affected. **Action:** Current issues mainly affect the web re-platform and here engagement with RMG security is being pursued through regular update meetings.

POL00338297

A24. Grapevine



Commentary

- There were 528 suspicious activities reported into Grapevine during period 4, bringing the cumulative total to 1667 year to date.
- There were 380 SMS blasts sent to 54,565 recipients during period 4, bringing the cumulative totals to 1246 SMS blasts and 188,298 recipients.
- 47 Police intelligence reports (5x5x5's) were sent to the Police during period 4, bringing the cumulative total to 180 year to date.
- The Grapevine database now contains 15861 entries.

Mitigating Actions, Update and progress

•Period 4 saw 506 additional Grapevine registrations, bringing the total to 4998 registered branches (7236 total members including Crowns and Supply Chain). The increase in registrations is largely due to recent multiple registrations and signup activity by the Fraud Advisors.

•Period 4 saw 168 calls from RoMEC for out of hours issues, a further increase on the previous month.

•The Taskforce operative with a crew from London Central made observations of a sus vehicle following a text blast, which were forwarded to Vanguard who were grateful for the intel.

•Following a text alerts, staff at various branches including Saltford BS31, Oldland Common BS30 & Aspatria CA7 received bogus phone calls from a male under the name of 'Colin' & 'Todd' requesting emergency cash for a customer. When the customers arrived, the spmr used delay tactics whilst contact was made wit the police on two occasions. Arrests were made at two locations.