

Security 4 Weekly Report 09/04/2010

HOT TOPICS:

Risks and Opportunities

Full year results

- **Fraud Casework** losses year to date amounts to £2.44m in 197 cases, an average loss of £12.4k
- **Supply Chain** losses year to date were £415.5k against a target of £850k which is £434.5k or 51.1% below target
- **Network** losses year to date were £1540.6k against a target of £1750.0k which is £209.4k or 11.97% below target
- **Weekly Incidents Report for first week -**



Weekly Incident Report 29Mar - 4th Apr 2010.zip

Significant Incidents (Network, Supply Chain or Fraud)

- **Network Robbery at Melsonby SPSO, DL10 5NF, on 23rd March.** Sub Postmistress fatally wounded after a robbery before opening time. **Loss £16.1k**
- **Network Robbery at Milltown SPSO, BT8 7SW, on 24th March.** Assailants dropped through the ceiling as the REM was being secured. **No reported injuries. Loss £75k.**
- **Robbery at Fleetville SPSO, AL1 4LJ, on 3rd April.** The office had closed but the retail shop was still open. One man wearing black clothes grabbed the retail assistant and forced the Subpostmaster to open the secure door, claiming he had a weapon. The Subpostmaster was preparing a cash remittance and the safe was open. **No injuries. Loss £67.6k**
- **CvIT Robbery at Drift Bridge SPSO, KT17 3LB, on 31st March.** After collection, at the CIT vehicle, two men demanded and grabbed the I-box. **No injuries. Loss £19k.**
- **CvIT Robbery at Thamesmead SPSO, SE28 8BG, on 31st March.** Delivery officer was grabbed from behind and threatened with a gun. The I-box was placed on the floor, which the attacker took and fled to a waiting motorbike. **No injuries. Loss £25k.**

Accomplishments

Casework Results

- **Starcross SPSO, EX6 8NY** - £16.1k Fraud Recovery
- **Richmond Road SPSO, KT2 5EL** - £14k Fraud recovery
- **Fowlmere SPSO, SG8 7SN** - £13.6k Fraud Recovery
- **New Cheltenham SPSO, BS15 1UL** - £9k Fraud Recovery
- **Stoke Newington CO, N16 7JN** - £7k Fraud Recovery
- **Barrow on Humber, DN19 7AA** - Defendant sentenced to 6 months imprisonment suspended for 2 years together with 220 hours of unpaid work.
- **Farndon Green SPSO, NG8 1DU** - Defendant sentenced to 12 month Community Order with a Supervision requirement.

- **Culverstone SPSO, DA13 0RQ** – Defendant sentenced to 120 days imprisonment suspended for 2 years with a Residence Order for 6 months.
- **Fishpool SPSO, BL9 9AX** – Defendant sentenced to 12 months imprisonment suspended for 2 years with a 12 month Supervision Order and requirement to complete 200 hours of unpaid work.
- **Downderry SPSO, PL11 3JZ** – Defendant sentenced to 180 days imprisonment suspended for 18 months with a curfew until 7 May 2010

Network arrests

- 2 men have been arrested in connection with a number of offences, including the armed robberies at Hensall SPSO, DN14 0QY, on March 4th, and at Owston Ferry SPSO, DN9 1RB, on March 16th.
- 2 males have been arrested following the attempted retail robbery at Moore SPSO, WA4 6UD, on 3rd April.

CViT attack arrests

- A male has been arrested and bailed in connection with the CViT robbery outside Clayton PO on January 19th 2010, however he has been subsequently re-arrested and remanded in custody in connection with another offence. A further male is still outstanding in connection with the Clayton incident, but is actively being sought by GMP.

Project & Programme update

Network

- In preparation for the transfer of the POL Hostage Helplines from Romec Arc to PWL on 19th April 2010, refresher training on the processes and procedures to follow has been given to the PWL Emergency Response Staff.
- Following daytime attacks on ten Post & Go machines across the Crown Office branch network, mainly in London, a number of meetings have been held with Wincor Nixdorf to identify solutions to the issue of the locking mechanisms which are able to be opened without keys on some machines. The supplier visited Trafalgar Square Crown Office on 6/4/10 and tried a temporary solution, but this was not successful. Lock re-alignment in two of the machines did correct the problem, but it is not known how long this will last. We are currently awaiting a formal recommendation from Wincor Nixdorf as to their proposals for a permanent solution to this issue. Communications have been sent to all Crown Office branches requesting that the note safe is defunded each evening and this appears to have had the desired effect as no further incidents have been reported since 29/3/10.
- **RoMEC:** Meeting held with Romec to explore ways in which we can develop cost effective security equipment solutions with greater emphasis on innovation by providing them with up to date risk information.
- **Collaboration with PFW:** Security engaged with Parcelforce Worldwide (PFW) to offer support and guidance in respect of driver and loneworker protection for PFW staff.

Supply Chain

- The inspection phase and subsequent draft report has now been completed into CvIT Depots and Cash Centres as part of Operation Ingress. A risk assessment is now being undertaken with regard to the recommendations made.
- **Mobile Billboard:** Deployment of the mobile billboard, advertising the businesses rewards policy, has commenced with visibility being given in high risk areas of Leeds. It is anticipated that this initiative will also be deployed around Manchester in the coming weeks.
- **Case Across the Counter:** Analysis in relation to the 'Case across the Counter' trial has been completed by the security team. Visits to the nominated offices are due to commence next week to view the sites physical suitability for inclusion.
- **CViT Home Office Meeting:** Security attended a meeting with Home Office Minister for Crime reduction for a meeting focussing on CvIT crime with other industry leaders.

Security programmes for products

- **ATMs** - Security, Network Support and the ATM Service Team met on 7th April to review 29 branches that regularly declare in excess of their maximum ATM cash limits. These branches are being targeted with intervention telephone calls by the Branch Performance Team. Use of this data stream and ongoing intervention/inclusion in the Branch Profile is also being explored.
- **POSS** - A conference call took place on the 1st April to discuss the content and messages to be included in the various communications articles that will be deployed to the network to support the migration of POSS onto automated card. A timeline for all communications has been agreed and the first operational focus article is due out on the 22nd April 2010, week 5. Both the Security Team and P&BA will be involved in agreeing all the final articles.
- **Stock Issues** - The Security Team have continued to work closely with Supply Chain and P&BA to explore the SAPADS system to try and extract information to develop a process to help P&BA reconcile stock remittances out of branch into Swindon. Initial investigations are positive and access to SAPADS is being requested for the Security Team to assist with future analysis.
- **Whistleblower** - As part of the ongoing fraud risk activities a new project is being undertaken for launch during 2010/11. A 'whistleblower' campaign is to be introduced whereby employees and associated third parties can communicate concerns about potential fraud and misconduct. A Project Initiation Document (P.I.D.) has now been produced and approved, with a Programme Plan setting out key milestones in preparation for launch.
- **iNet2Door** - The business is developing a new service whereby customers can order certain items on-line and arrange to pay for and collect from Post Office branches. This service is to be run as a pilot across 700 branches within the M25 and requirements are currently being agreed. The Security team have provided

requirements around payment, identification, storage, collection and monitoring of fraud risks to ensure the pilot is successful. If the pilot is successful, which is due to run until the end of year, full roll out will take place around April 2011.

- **DVLA** - The relationship continues to develop with a number of recent successes with branches and DVLA issues. Two recent branches have identified persons involved in criminal activity which has resulted in reductions of manual transactions. A number of communications are to be deployed across the DVLA Network over the coming months. These are top tips devised as a result of the improving business partnership with DVLA.
- **AEI** - The new AEI (application, enrolment and identity) booths currently on trial are to be further rolled out to branches. One risk has been raised by WHSmith around any possible increased risk of attacks due to the AEI booth being closed in on 3 sides, with the remainder facing the counter position.
- **Camelot Receipting** - The current manual process for managing prize payments is to be replaced by an automated system driven solution. The levels of non compliance in this area are high, although fraud is minimal. The branches receipting templates and customer information requirements have generated the greatest discussions and work with product and compliance is ongoing with Camelot to come to a workable solution to all.
- **Horizon Online** - As part of the cash verification activities associated with migration, in particular any potential fraud issues, Security and P&BA will continue to monitor all branches pre/during/post migration.
- **FONCH (Foreign Overnight Cash Holdings)** - Work is ongoing to produce the reconciliation and discrepancies. It is been agreed that a business project should be raised to resolve the wider issues on this, with full support from security and analytics.
- **Spoilt Postage and Rejected Labels** - A meeting has taken place between the Security Team, Business Efficiency and P&BA to scope the possibility of embedding phone call intervention activity at P&BA as business as usual. Process recommendations will then be made via the Fraud Forum for feedback and a decision in relation to introducing this process will be made in collaboration with the appropriate stakeholders.

Business Programmes, Security Issues

- The delay to the new eBusiness Portal means the Group as a whole will not be ready for a full PCI audit across the group for December 2010. This will need to be carefully managed with the acquirer.
- Positive engagement with RM Information Security to get RM PCI programme properly started. They have done a good deal of background work for us. RM PCI Programme now beginning to take shape.
- Detailed Programme Plan produced but this requires further work to define stakeholders, owners and meaningful timescales.
- The programme library has been created and is now being populated. Need to agree who needs access to the library.

- We now have the details around the RMG Telephony Project.
- Contact has been made Clare Taylor in Tallents House to discuss ongoing IT Projects and PCI Compliance
- Roll out of the Royal Mail course, '**Conflict Management/Disengagement Physical Intervention Skills**' has commenced. A large number of POL Security Advisors will be undergoing this training.
- **Financial Services Specialist** - Since the introduction of laptops for FSS's, 15 of those laptops have been stolen, we are in discussion with Commercial Security to determine what steps can be taken to reduce this, and to decide if 'laptops' are the right equipment for the job.
- **Insurance** - There are a number of incidents on both over 50's insurance web site and motorcycle insurance web site - these are low volume products, but the problems are symptomatic of poor performing 3rd parties and could have a knock on effect to other direct channel products.
- **POca** work continues around POca2 and the Holly Contract.
- **SMOTS** (simple money transmission service) - security plan development is almost complete.
- **IPS** tender preparation is underway.
- Progress has been made with Fujitsu in moving towards the delivery of evidence to support acceptance, although there is still considerable work to be done in the area of patch management. The work on risk assessment is continuing and is likely to deliver an acceptable plan, but this is at the expense of the longer-term ISO27001 certification strategy. It appears there is a lack of suitable resource within Fujitsu including the failure to have found a replacement Security Architect.
- Projects in which we have had involvement are continuing to progress and collaborative working with the likes of Service Delivery is continuing.
- The work on the E&Y audit is virtually complete, other than dealing with the feedback and observations.
- There continues to be an increasing demand on resource from projects which are typically requiring responses turned-around in less than a week to some complex issues.

Security Team