POL00423197

In Confidence

Fraud, Commercial and Information Security Review 2009/2010

Post Office Ltd

POL00423197

In Confidence

Contents

POL00423197

In Confidence

3.2.1.2 Post Office Savings Stamps (POSS)

3.2.1.3 Lottery Scratchcards

3.2.1.4 Alliance and Leicester Business Deposit Reversals/Suppression

3.2.1.5 Christmas Club Card

3.2.1.6 Bureau De Change

3.2.1.6.1 Foreign Exchange

3.2.1.6.2 Foreign Over Night Cash Holdings (FONCH)

3.2.1.6.3 Counterfeit Currency

3.2.1.6.7 Travel Money Card (TMC) Chargebacks

3.2.1.6.8 Moneygram

3.2.1.6.9 Travellers' Cheques

POL00423197

POL00423197

Fraud, Commercial and Information Security Review 2009/2010

Introduction

This report provides a detailed analysis of Fraud, Commercial and Information Security risks for Post Office Ltd, including the Supply Chain. It describes the Security Team activities to minimise risks appropriately, to enable Post Office Ltd to operate a secure environment in which to conduct service and deliver products through all channels. The management summary highlights the high-level risks, with the detail contained in the body of the report.

Executive Management Summary

1 Business Losses

Underlying losses for 2009/10 are circa £15m (net losses lower due to credit posted from provisions posted in earlier years), this includes new provisions for cash remittances including Foreign Currency.

2 Fraud Casework

2.1 Casework overall losses (£2.44m), numbers (197) and average case loss (£12.4k) have all reduced year on year.

2.2 The majority of casework losses £1.8m (74%) were due to audit deficiencies.

POL00423197

2.3 The recovery rate was 79% with £2.2m recovered from losses of £2.8m in closed cases.

3 Fraud Risks and Security Programmes

3.1.1 Crown Office Losses. A Security programme to address these targeted a reduction to £1.42m (to improve on the loss budget of £1.78m), the final out turn was £1.64m.

3.1.2 Cash Issues. Cash held in the network and the false accounting of that to cover fraud remains one of the major fraud risks. At year end, in those offices over target, there was £32m excess to holdings, in which fraud can be hidden. Non-conformance to ATM cash reporting presents further cash risk in the network.

3.1.3 Stock Issues. The misuse of the stock adjustment function on the Horizon system exposed the business to £2.6m of claim from Royal Mail in the previous year for alleged sales. Work undertaken this year to prove claims are due to accounting error will allow claims to be challenged. It emerged that poor controls on remittances in and out of Swindon stock centre allow over-claim and fraud. Although to date only circa £200k in fraud cases has arisen the scale and time-line means that unrecoverable fraud loss will have occurred and the potential is wide ranging.

3.1.5 Payment card issues. These surround the controls in place to mange customer information securely and limit fraud through channels. Post Office Ltd has made good progress towards being Payment Card Industry (PCI) and Data Security Standards (DSS) compliant in respect of customer data. To limit fraud through channels, Cybersource and 3-D Secure in addition to other verification processes and the removal of the signature fallback for cards has ensured levels remain below the 1% fraud target limit for schemes.

POL00423197

3.2 Product Pillars

3.2.1 Financial Services. At office level fraud has been perpetrated by false accounting and inflation of ATM cash (£127k) and Lottery Scratchcards (£221k in cards, total losses £480k) to conceal fraud. Over-claims have been made on Post Office Saving Stamp redemptions to the value of £800k that has been recovered by issuing Transaction Corrections. Issues with Foreign Currency accounting issues have resulted in a provision for £1.1m.

3.2.2 Government Services. Low levels of fraud, but key to client engagement, has been managed for both Post Office Card Account (POCA) and DVLA this year. New initiatives Simple Money Transmission Services (SMoTS), Application, Enrolment and Identity (AEI) and Immigration and Passport Services (IPS) have all had Security input.

3.2.3 Mails and Retail. Rejected and Spoilt Postage Label fraud (£92k avoided losses known from stock reduction and transaction corrections issued) has been managed down to a level that intervention activity can be transferred to other teams for containment. A Mails Integrity programme continues, to ensure all offices become Mail Integrity compliant in the coming year.

3.2.4 Telecoms. Telephony bad debt write off this year amounted to £3.8m, with levels currently at 6% compared to Industry levels of 4% to 10%.

4 Information Security Risks and Business Projects

Invitations to Tender (ITT). Security input to Merchant Acquirer, Prepaid Card and Cheque ITT this year.

Business System changes. Security working with the Connect 2010, Web re-platform and Horizon Online projects to ensure secure deployment.

Governance Projects. Relationships and requirements for standards are being driven by a number of governance projects, including the Bank of Ireland (BOI)/Post Office Financial Services (POFS) Governance and Government Security Policy Framework (SPF), into which the Security Team are providing input.

5 Emerging Risks, Threats and Initiatives 2010/11

Losses management. A programme to deliver 10% reduction in losses and governance is set to deliver next year.

POL00423197

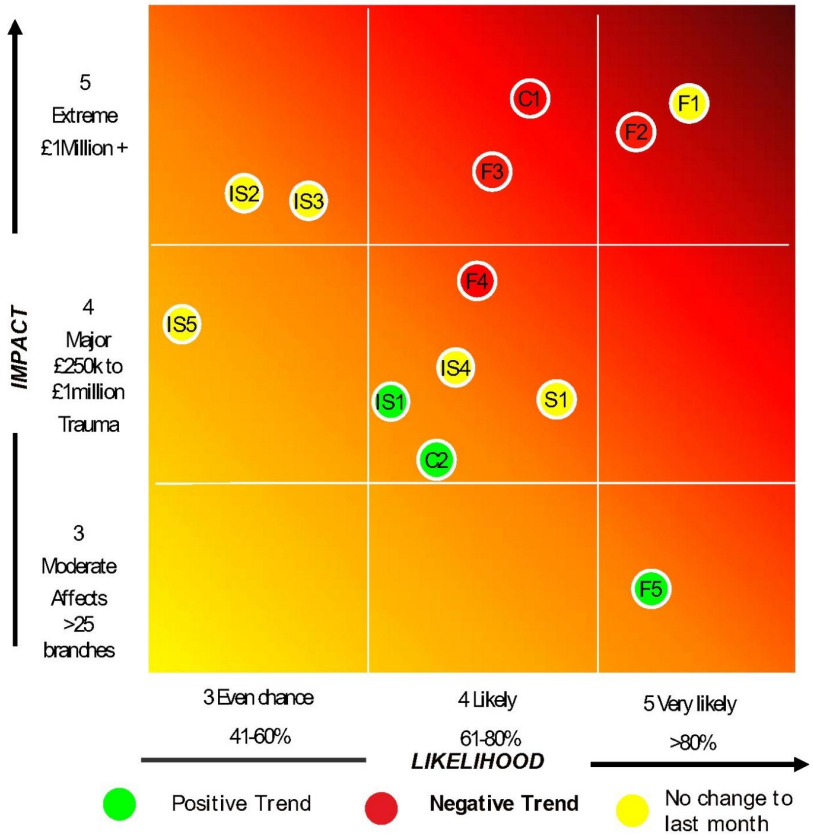
Fraud management. Maximising Intelligence, Management Information and Grapevine Intelligence services in the next year is intended to deliver better risk focus and includes the launch of a Whistleblower line

Information Security Risks

Attacks on Post Office Ltd systems and information, including malicious web activity, phishing and spam, and targeted attacks on identity and payment cards details are considered to be the predominant risks in the coming year.

POL00423197

Risk Matrix



Fraud Risks

F1 ONCH inflation of Cash In Tills (offices over target are over holding £32m)

F2 FONCH provision of £1.1m from branches holding less than Post Office Ltd accounts (includes fraud). £2.6m written off against previous years credits for stuck items.

F3 Crown Office Losses including fraud £1.64m> target of £1.42m

F4 False accounting of stock (Inc Savings Stamps, Scratchcards & Hemel issues)

F5 RM Revenue Theft, Rejected and Spoilt Postage Labels (non cash impacts)

Commercial Security Cash Loss Risks

C1 Telephony bad debt inc fraud (£3.8m full year write off)

C2 Sterling Counterfeit (£347k write off full year compared to £597k last)

Security Cash Loss Risks (Combined Physical & Fraud)

S1 ATM Crime (Rob, Burg & Fraud)

Information Security Risks – Non Cash Impacts

POL00423197

In Confidence

IS1 RMG fail to deliver IS responsibilities (when Post Office Ltd dependent)

IS2 Non-Compliance to IS policies

IS3 Data on removable media lost or stolen

IS4 Counter Transaction process control failure

IS5 Non compliance to PCI/DSS Track 2 requirements

POL00423197

In Confidence

1. Business Losses

Commentary: Underlying losses for 2009/10 are circa £15m (net losses lower due to credit posted from provisions posted in earlier years), this includes new provisions for cash remittances including Foreign Currency. The manner in which losses are accounted for across the business is both complicated and lacking in robust governance, making it difficult to forecast losses with any real degree of accuracy and ultimately target activity to drive down the cost of losses across the business.

Mitigating actions, update and status

A Business Efficiency programme has been established with the following aims:

- To provide a focal point for losses across the business
- To clean the loss budget data and release funds if the budget is excessive
- To reduce the total cost of losses across the business
- To identify and evaluate areas of potential loss reduction

The programme has commenced, however the returns will not be realised until 2010/11.

2. Fraud Casework

2.2 Numbers and Losses

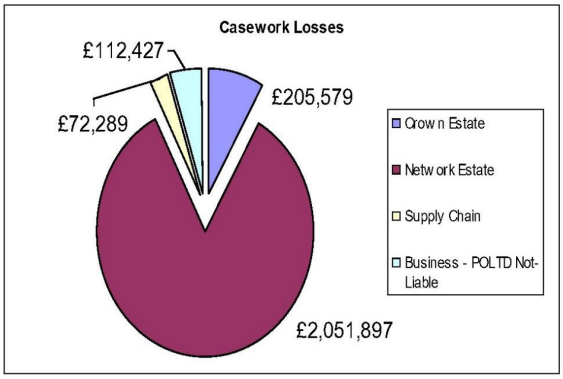
There were 197 fraud cases raised during 2009/10, which was 15.8% fewer compared to 2008/09 at 234 cases.

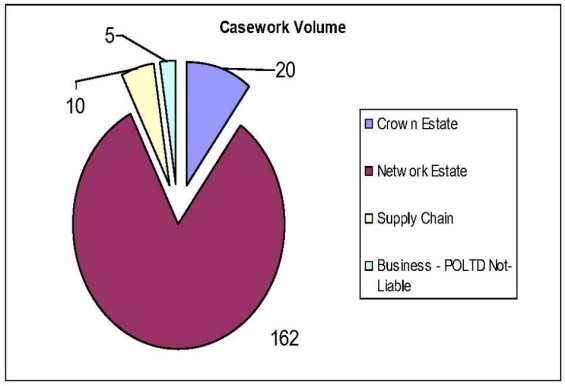
Total casework losses for 2009/10 amount to £2.44m in 197 cases with an average loss of £12.4k compared to £3.96m in 234 cases with an average loss of £16.9k during 2008/09.

There were 10 Supply Chain fraud cases with a total value of £72,289 and average loss of £7.2k, compared to 7 cases totalling £66,953 with average loss of £9.6k during 2008/09.

POL00423197

In Confidence

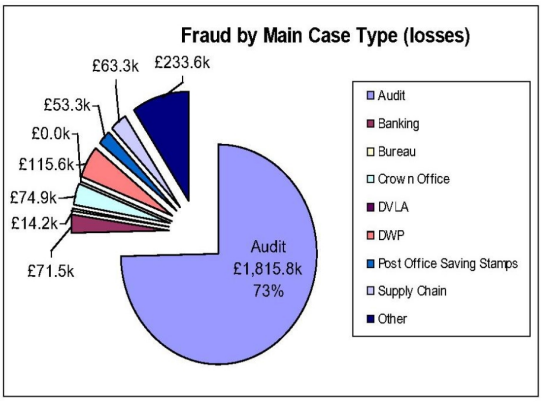


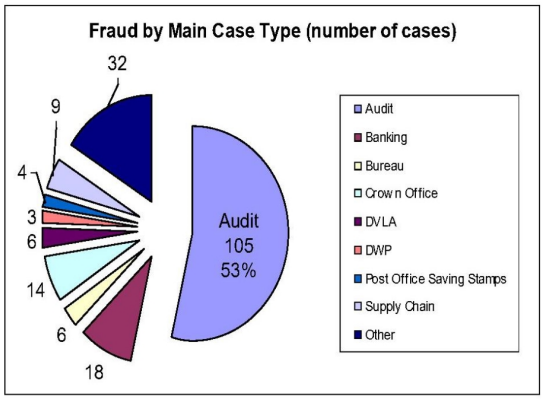


POL00423197

2.2 Audit Shortages

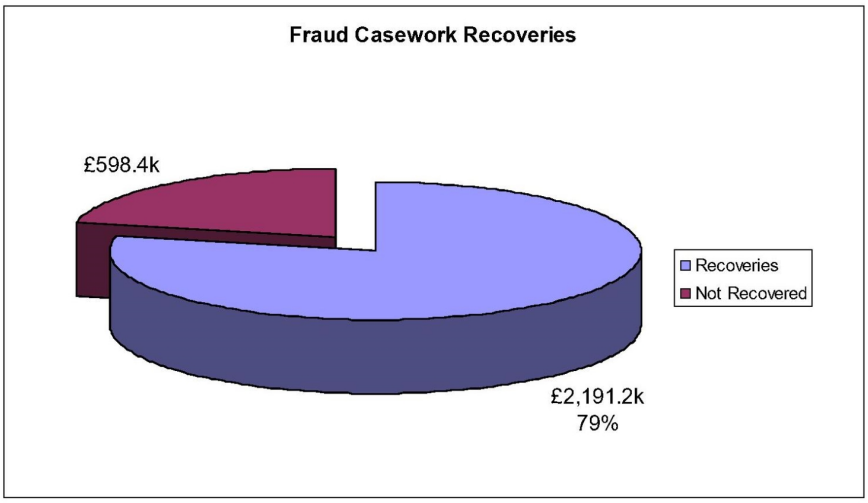
Audit deficiencies account for £1.8m (74% of losses for all casework raised) in 2009/10, compared to £2.98m (75% of all casework raised) during 2008/09. Average audit losses stand at £17.3k per case in 105 cases raised in 2009/10 compared to £26.6k in 112 cases during 2008/09





2.3 Financial Investigations Recoveries

From all cases closed, year to date £2.2m has been recovered against identified losses in those cases of £2.8m. The recovery rate for 2009/10 is 79%

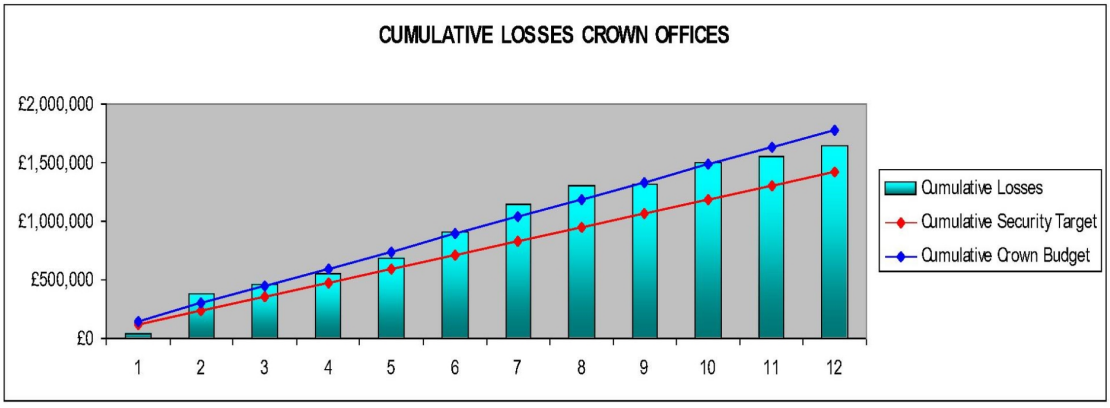


POL00423197

3. Fraud Risks and Security Programmes

3.1 Operational Risks (Channel, Inventory, Method of Payment, Accounting)

3.1.1 Crown Offices Losses



Security objective: Support the Crown Office estate to achieve budget for losses in 2009/10 (£1.78m), with a Security aspiration to reduce Crown Office losses by a further 20% (£1.42m).

Result: At year end, losses posted to the accounts totalled £1.64m, within Crown budget but in excess of Security target (13%).

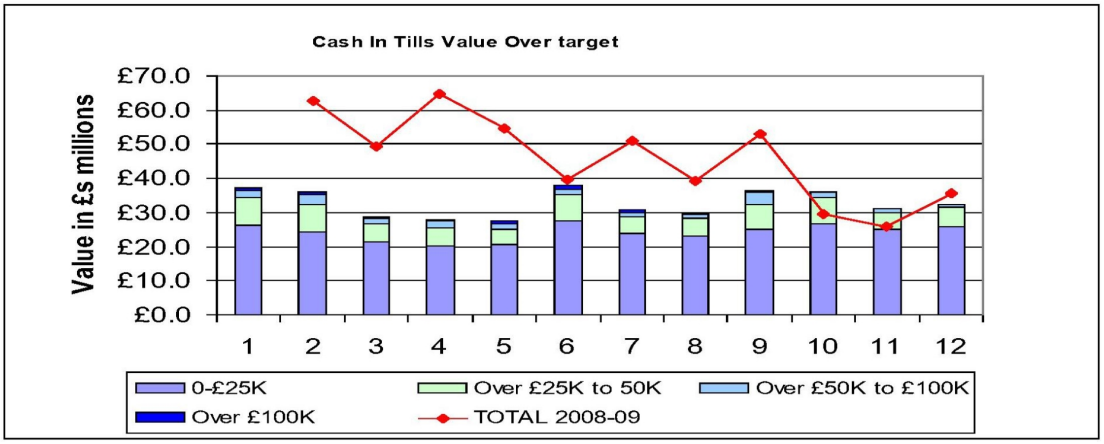
Programmes: Toolkit drafted and utilised by Security Team to address 50 worst performing branches. These branches sustained a £50k improvement during the implementation of the Toolkit programme. Close working relationship with Business Efficiency and other Stakeholders in relation to Crown Losses Review and other areas affecting losses. Increased communications via Crown Focus and TV Screens, ensuring Security messages are relayed to branches.

2010/11 Proposals: Expansion of the Toolkit to include all Crown Offices, attend CAM/BM meetings, continued implementation of Business Efficiency recommendations, ascertain root cause analysis of losses, deployment of revised/simplified Losses & Gains policy, and further utilise communication channels. The loss budget has been set at £1.61m, though the Security Team have set their target at £1.47m (representing a 10% reduction against 2009/10 losses).

POL00423197

3.1.2 Cash Issues

3.1.2.1 Cash Inventory - Over Night Cash Holdings (ONCH)



Security objective: Reduce ONCH in general across the Network and identify, then deal with ONCH related fraud risks through a programmed approach.

Result: At P12, cash at branches over target was £35.2m. There have only been two periods where ONCH levels were higher than the same periods last year (a contributory factor being Operation Hogmanay in 2008/9, whereby in P10 and P11, £15m was returned to the business). Across 2009/10, there have been 8 periods of positive ONCH trend against targets, 2 periods of no change and 2 periods of negative trend.

Programmes: Operation ONCH 300 focused on 300 branches holding excess cash and a phased programme of intervention (letters, telephone calls and visits) resulted in £1.5m being returned to the business. Operation Sunshine focused on 200 branches holding excess cash and similar phased intervention resulted in £5m being returned to the business. Additionally, 7 cases of fraud were identified with losses of £300k. These programmes, along with other Stakeholder activities, have seen major reductions in the volumes and values of fraud cases in 2009/10.

2010/11 Proposals: Cash inflation and false accounting still constitute high fraud risks and further operational programmes are planned. A business as usual approach is also being explored during periods where there are no ONCH programmes running, utilising robust data streams with a view to targeting a number of branches each month.

POL00423197

3.1.2.2 Cash in Pouches and Remittance Reversals

Modus Operandi: Fictitious cash remittances can be created (inflating cash in pouches and suspense accounting figures) reducing cash on hand needed to balance the accounts, then reversed before despatch. Also cash despatches can be held back allowing for more cash to accumulate before despatch or being held in pouches. The amount will be held as cash in pouches on the branch trading statement to cover up a cash shortage, known as suppression.

Programme: A trial of 10 test audits, resulted in no significant losses. Analysis is now being passed monthly to P&BA to perform business as usual checks on branches showing unusually high numbers of reversals. Branches of concern will be escalated to the Security Team, to make a decision as to the appropriate course of action.

3.1.3 Stock Issues

3.1.3.1 Stock Adjustments:

Modus Operandi: Stock levels are increased using the stock adjust function to hide cash losses. This reduces the amount of cash needed to balance the accounts.

Commentary: Postage stock adjustments resulted in a settlement discrepancy of £2.6million to Royal Mail in 2008 / 2009 whilst this year Post Office Ltd are discussing what, if any, amount is due now a clear audit trail is provided. Throughout this financial year P&BA have contacted branches making stock adjustments on a daily basis and have requested that they correct non-conforming adjustments through reversals or sales.

Programme: An Audit Command Language (ACL) programme has been introduced to manage stock and allow P&BA to target offices more efficiently, with a clear audit trail providing evidence that adjustments have been dealt with.

3.1.3.2 Stock Remittance Issues:

Modus Operandi: Offices are able to receive stock remittances from Swindon stock centre without booking this into the branch accounts and can also book in less than is received. Cash from sales of this stock can be misappropriated. Branches can also book out non-existent stock to Swindon or over inflate the amount of stock returned, thus showing a gain in the branch accounts, which can then be removed. In both

POL00423197

cases robust procedures for identifying discrepancies in these processes have been virtually non-existent since 2007.

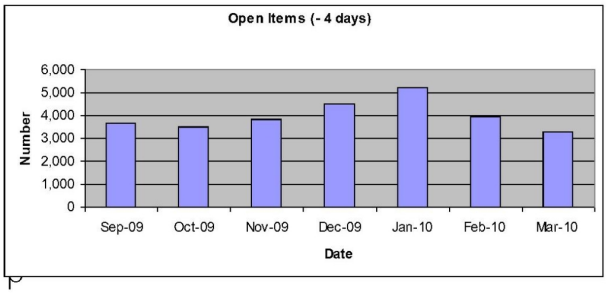
Commentary: There have been two investigation cases with losses totalling £21,000 in respect of offices not booking in stock despatched by Swindon. There has also been a case raised at a branch that has been both inflating stock remittances to Swindon and booking out non-existent stock. This case alone stands at a loss of around £170,000.

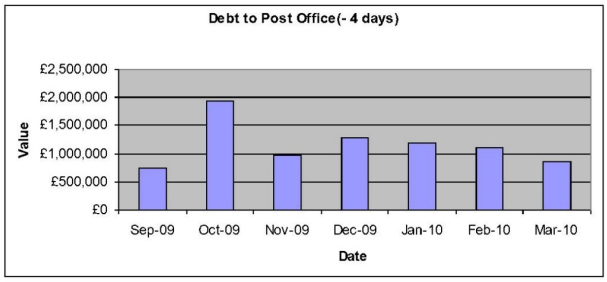
Programme: A programme to encompass all stock remittance processes and reconciliation between Swindon and P&BA is now under way. A new ACL programme has been built to allow P&BA to reconcile the amount of stock booked out of Swindon with the actual stock booked into branch. During the test period for this programme transaction corrections totalling £5500 were issued to branches who had failed to book in stock from Swindon.

2010 / 2011 Proposals: The Security Team will be working with all appropriate stakeholders during the next financial year to ensure that the gaps identified are mitigated and that processes between Swindon and P&BA become both robust and consistent.

POL00423197

3.1.4 Cheques – Open Items





Modus Operandi: Cheque processes facilitate fraud by allowing inflation of accounting figures of cheques on hand at a branch, branches can also over-claim or suppress their submission of cheques.

Commentary: By year end, open items reduced by 32% from 4,809 in March 2009 to 3,292, with a balance due to Post Office Ltd down to £865,642 compared to £2.4 million in March 2009. There have been no outstanding items over four months old throughout this year.

Programmes / Mitigating actions: P&BA continue to contact branches on a daily basis as part of business as usual intervention activities with the Security Team providing a monthly feed of analysis to assist in this activity. The Security Team and P&BA have been involved in the recent cheque tendering process to ensure all aspects of the process are covered.

2010/ 2011 Proposals: Continued business as usual intervention activity by P&BA. Liaison will take place with the chosen processing partner, ensuring that the necessary information files are supplied to P&BA to enable efficient management of open items. As the balance and levels of open cheques are at an all time low consideration will be given to setting a tolerance level.

3.1.5 Credit / Debit / Prepaid Card Fraud- Chargebacks

3.1.5.1 Payment Card Industry (PCI) - Data Security Standards (DSS)

Issue: Post Office Ltd processes over 6 million card transactions annually, thus as a Level 1 merchant for Visa and MasterCard, should not retain sensitive payment card

POL00423197

information in Post Office Ltd systems after payment authorisation. The Track II data stored by Post Office Ltd under an old version of the LiNK interface makes the business non-compliant and liable to potential fine of £417.8k for a 24 month period. The PCI DSS audit of 229 PCI Controls returned a 68% pass rate. Primary failure was patch management and anti-virus, but once fixed and 45 controls checked, expected result is 93% compliance.
Mitigating actions, update and status: There are no findings against which Post Office Ltd cannot mitigate against any concerns our Merchant Acquirer may have. Post Office Ltd have been found to be over 60% compliant (the standard requires either 100% or the existence of agreed "mitigating controls"). It is understood that this level of compliance is well ahead of other comparable UK organisations. The PCI Project has produced a BAU SLA for Service Delivery to implement with Fujitsu, to show regular repeatable security activities that provide evidence of compliance to the PCI DSS standard. Track II data in the historical audit log remains a problem to be resolved, though the new version of LiNK is PCI DSS compliant.

3.1.5.2 Technical Fallback

Fallback is allowing a chip and pin card to "fallback" to swipe and signature: once the chip has failed 3 times, the customer should not sign the receipt, but should be requested to pay using an alternative method. However, until September 2009, Post Office counters were allowing this type of transaction. Almost all UK issued cards are now chip, therefore Visa and MasterCard advice that Post Office Ltd must use chip and pin only and staff should not allow transactions to "fallback" to signature if the cards have Chip and Pin capability. However many foreign cards are still not Chip & Pin, yet there is no shift in liability for those foreign magnetic stripe cards. As the business observes the "Accept all" rule, that might translate into a chargeback problem.
Mitigating actions, update and status: Work is ongoing with P&BA to implement a control mechanism to monitor card activity. Prevention of "fallback" use on swiped chip card transactions has resulted in a reduction in chargebacks of £204k this year against £467k last.

3.1.5.3 Card Not Present (CNP)

POL00423197

Post Office is at risk across its internet and call centre services from CNP transactions. These channels require diligence in fraud control efforts. The 3-4 digit security number (CVV2) is used as a way of defining customer profiles and another fraud prevention tool for online transactions is "3-D Secure", the industry standard defined by Visa and MasterCard. Ultimately, the risk of CNP fraud lies with Post Office Ltd, so it is important to provide the necessary tools to protect the business, by managing and reducing the exposure to fraud, chargebacks and associated costs. Mitigating actions, update and status: 3-D Secure authentication should be used in conjunction with existing fraud checks such as Address Verification Service (AVS) and CVV2 to help further minimise the risk of fraud. Chargebacks can still occur even when transactions have been fully authenticated by 3-D Secure, but this year they amounted to £24k when that system was switched off between August and September 2009. Chargebacks are carefully monitored by both the Security Team and P&BA to ensure that the level of fraud does not exceed 1% of total card transactions to avoid industry fines. The PCI programme has defined call centre audits and scheduled an engagement with service delivery to get the activity underway. Some remedial work has been done to address CSC Portal risk due to unencrypted card data transmission, contrary to PCI DSS requirements. The PCI DSS programme proposed Royal Mail Group implementing the same BAU SLA developed for Fujitsu to check, an on-going basis, the status of the security and the level of compliance being maintained. The PCI DSS programme is not involved in the new eBusiness platform because Royal Mail Group IT feel they have adequate expertise within to cater for PCI DSS. There is a risk on the late delivery of the platform that will be mitigated by the PCI DSS programme providing evidence of compliance in the other card acceptance areas.

POL00423197

3.1.5.4 Cybersource

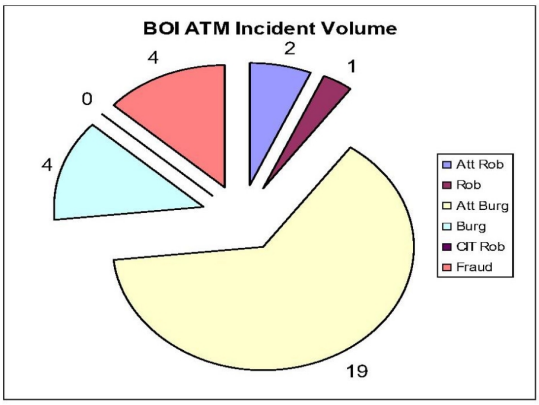
Cybersource Decision Manager is fraud mitigation software designed to protect Post Office Ltd products that are available online or through call centres. It checks for suspicious transactions and compares them against Internet Protocol (IP) address verification, global telephone directories, global delivery address verification services and positive and negative lists. Currently, there is no contract in place and the relationship is managed through monthly purchase orders. There is not an effective process in place for the management of this software and until recently there was no user guide either.

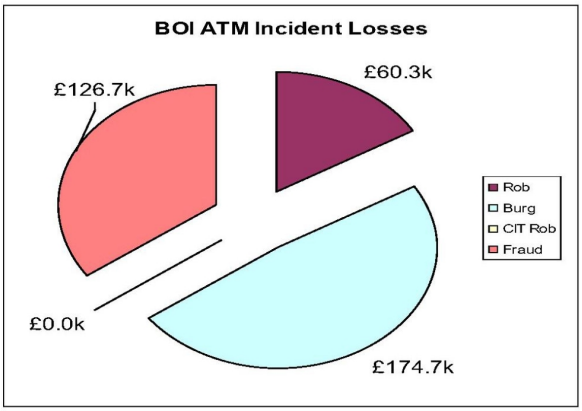
Mitigation Actions: The Security Team provided budget to enable representatives from Web Support, C&IS and Security to be trained in order to manage the software tool effectively. Further training for BOI and FRES was delivered to ensure Cybersource rules were communicated properly. The Security Team and C&IS completed a user guide to ensure those rules are recorded and communicated to all stakeholders, which once feedback is received and addressed, will be added to the library for future audits.

3.2 Product Pillars

3.2.1 Financial Services

3.2.1.1 ATMs





Total Bank of Ireland ATM security-related losses for 2009/10 amount to £361.7k from 30 incidents, compared to £994.1k from 28 incidents last year. Whilst there is an increase of 7% in volume, there was a 63.6% reduction in losses.

POL00423197

During 2009/10, there were 4 fraud-related ATM cases accounting for £126.7k, 4 burglaries at £174.7k, 1 robbery at £60.3k, and 19 attempted burglaries and 2 attempted robberies.

Mitigating Actions: The Security Team worked closely with the ATM Installation Team throughout the year to ensure that security standards are fully complied with during all ATM installations and recommended security upgrades, identified on the ATM High Risk Matrix, are duly installed. Fogging systems introduced into high risk branches, where four activations have potentially saved £440K against an installation cost of approximately £8K. Temporary fogging kits were deployed into the Bradford area to mitigate against a series of ATM-related attacks and additional GPRS alarm kits were purchased to improve the ability to mitigate against line cut activity. Romec ARC continues to notify Grapevine of 'out of hours' line cuts at ATM sites so as to facilitate a timely response to all such incidents.

Cash Management have allocated ATM targets in the past year, with remittances standardised to reflect this, whilst an 'ATM Viewer' software tool is used to calculate cash requirements based on previous ATM usage. Special requests by branches for an increase/amendment are challenged more vigorously and proactive contact with branches will continue, as will programmes to specifically tackle ATM holdings and ONCH.

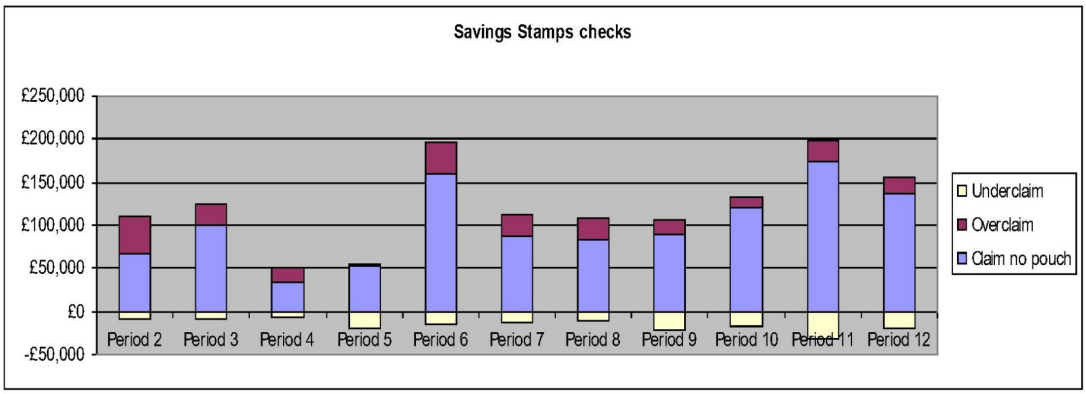
2010 / 2011 Proposals: Re-designed ATM Security Forum will ensure key stakeholders are brought together to identify and focus on addressing key ATM related issues. Pro-active use of temporary fogging and alarm kits will provide a strategic response to emerging risks.

A number of bulk audits/cash verifications have been requested at branches with high ATM holdings, as ATMs are excluded from HNGX migration checks. Monthly Interventions commencing, in partnership with Cash Management, based on ten data streams, including ATM holdings. Further stand-alone programmes are planned to target numerous branches and undertake a phased approach to securing cash returns and identify fraud.

3.2.1.2 Post Office Savings Stamps (POSS)

POL00423197

In Confidence



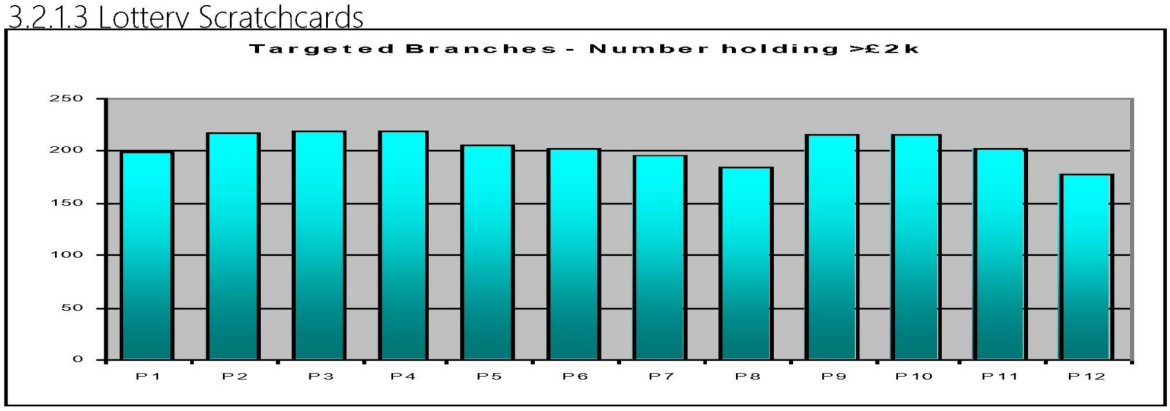
Modus Operandi: External fraudsters can transact counterfeit stamps or internal fraud by stock theft and re-introduction into the pipeline. Internal staff can over-claim or make fictitious claims in relation to the amounts of POSS redeemed through their branch. A P&BA report indicates over £800k p.a. is lost due to branch malfeasance.

Mitigating Actions: Continuous monitoring of the product (50% physical checks) and a risk-based targeted approach to the problem involving investigations, phone calls and the issuing of transaction corrections. A case involving the sale of POSS on E-bay resulted in the recovery of £169k through stamps stolen from Hemel Hempstead stock centre. The offender, a Royal Mail employee at the time the centre was under their remit, was prosecuted and received an 18 month custodial sentence.

2010 / 2011 Proposals: The business case was agreed to replace the current product with a pre-paid budget card (modelled on the Christmas savings card and risk-assessed by the Security Team). The migration date is now confirmed as the 25th May 2010, with the Security Team working with P&BA and Swindon to mitigate the potential risks concerning redemptions and returned stock.

POL00423197

3.2.1.3 Lottery Scratchcards



Modus Operandi: Losses relating to scratchcards reflect a mix of non-compliance and fraud; sales are not entered into Horizon which indicates artificially high holdings, scratchcards are inflated to conceal losses within the accounts, stock holdings are not adjusted when Transaction Corrections are received, cash from sales is not physically transferred to the branch, cash is not transferred on a daily basis, expired scratchcards have not been returned.

Security Objective: Manage fraud risk processes for excessive Scratchcard holdings, aiming for a £2k maximum stock holding at branches, implementing intervention strategies as appropriate.
Result: Approximately 3500 branches sell Scratchcards and an average of 204 branches each month hold more than £2k (only 6% of all Scratchcard branches). At P12, 178 branches held more than £2k, the lowest number of branches this year.
Programme: 39 Scratchcard-related audits have been requested this year, identifying £480k of losses, of which £221k related directly to Scratchcard concerns. Intervention activities (telephone calls/visits) have been undertaken by Security at 90 branches, communications via ONCE pouches have been targeted at 500 branches and details of all branch holdings in the network are relayed to appropriate Stakeholders every month.
2010/11 Proposals: Continuation of business as usual activities; intervention visits (Network Support), telephone calls (NBSC) and targeted communications (Security) to branches. Implementation of PING reporting, led by Business Efficiency, to provide better MI and reduce avenues for fraud. Exploration of new monitoring and targeting

POL00423197

based on number of dispensers/inserts at branches, rather than a blanket £2k holdings target. To consider wide ranging audit activity at offending branches, in addition to monthly BAU targeting.

3.2.1.4 Alliance and Leicester Business Deposit Reversals/ Suppression
Modus Operandi: Business deposits are suppressed to hide losses; these may be reversed out of Horizon showing an audit trail for analysis.
Mitigating Actions: Monitoring including reversal activity takes place to gauge risk levels. Risk reduced by the introduction of the automated card for the majority of business customers, as these cannot be reversed without NBSC authorisation.

3.2.1.5 Christmas Club Card
Modus Operandi: The risks centre on the possibility of forging/counterfeiting the magnetic strip cards, which could result in customer savings being withdrawn fraudulently. Further risks have been documented around the processes for loss or theft of cards, or alleged loss or theft or repayment of funds, allowing customers to obtain duplicates or return of funds twice.
Commentary: Despite the risks identified, no fraudulent activity has been reported or identified during this year.

3.2.1.6 Bureau De Change
Total loss across Bureau products (including card fraud chargebacks) was £204k, compared to £467k last year, primarily due to branch non-conformance on Method of Payment (MOP) acceptance.

3.2.1.6.1 Foreign Exchange
Modus Operandi: Reversal transactions are an indicator of fraud where transactions are reversed from Horizon, allowing the margin (the amount Post Office Ltd gets from any buy and sell transaction) to be stolen. What is more difficult to identify is when margin theft is not processed through Horizon (neither buy nor sell transaction).

POL00423197

Commentary: No robust evidence from the current analysis has identified a major issue.
Programme: Initial data around reversals was easy to identify and produced data across almost every branch in the Network, including branch breakdown of reversal data in a league table. Business concerns about this issue were communicated to the network. The Security Team are working on a model to try and identify branches where Horizon is by-passed completely. This involves a complex indexing system, using traffic data from previous years, but the results can only flag a potential issue, rather than provide evidence.
Result: The levels of reversal transactions have gradually declined. There are genuine reasons for reversals but, given those, reversal numbers should be relatively small. The problem with all Bureau anomalies is the scale of the transaction volumes and values. Reversals have seen around a 12% reduction over the period of the year.

3.2.1.6.2 Foreign Over Night Cash Holdings (FONCH)
A sum of £1.1million was provided for in the year end accounts, to cover the discrepancy between the POLFS accounting system and the figures held in branches on Horizon. Although initially the discrepancy levels and unknown cause gave concern, for the ability to reconcile, limit losses and identify fraud, it now seem likely that the root cause has been traced to a back-office system migration that can be quantified and rectified, albeit this will result in a loss to be written off. Work is ongoing at P&BA to obtain the data necessary to quantify the discrepancy and reset POLFS.

POL00423197

3.2.1.6.3 Counterfeit Currency

A number of cases, where offices had acted non-compliantly in re-circulating high value foreign currency notes, resulted in customers being issued with counterfeit currency. This came to light in high profile cases when two individual Post Office Ltd customers were arrested abroad in receipt of this counterfeit currency. Individual clerks and branches are to be dealt with using existing disciplinary and contractual routes and a re-iteration of the correct operating procedures is due, before the main travel season.

3.2.1.7 Travel Money Card (TMC) Chargebacks

Modus Operandi: Travel Money Card is a simple magstripe card, quickly overcome by fraudsters.

Commentary: The loss figure for 2009/10 is only £24k and the majority of this loss occurred when business switched off 3-D Secure and Cybersource between August and September 2009. This was due to e-business advising of severe problems in the web channel which required a payment module fix.

Mitigation Actions: 3-D Secure and Cybersource' s ID morphing rule have worked well since September 2009. As a result of this Post Office Ltd, FRES and BOI were confident that in order to increase sales on Travel Money Card, the Experian Score for "Know Your Customer" could be reduced from 60 to 50, since any abnormality would be spotted by Cybersource and addressed immediately by the business. BOI and FRES have since reported a 20% increase in sales. It was decided that the Fraud liability on TMC sits with BOI.

3.2.1.8 MoneyGram

Modus Operandi: Since the previous year' s approximate £500k write-off the business has presented evidence to Moneygram to support the reimbursement of approx £250k. Discussions between Post Office Ltd and Moneygram have led to an initial offer of half the amount and Post Office Ltd is negotiating an increase in the offer.

Commentary: Since automation of the transaction on Horizon, the business has not been exposed to any fraudulent activity. This product' s Method of Payment (MOP) is

POL00423197

cash only and all fraud risk liability is owned by MoneyGram. There is no fraud reported/identified to date on this product.

3.2.1.9 Travellers' Cheques

Commentary: In 2009 a comprehensive analysis was carried out by the Security Team to reduce fraud on Bureau products and according to the evidence there is no specific branch or location that has been targeted by fraudsters on a regular basis.

Mitigating actions, update and status: There are already robust fraud measures in place, encashment requiring Amex authorisation of bar-coded cheques. However, the Security Team will continue to monitor the Travellers' Cheques on a day to day basis with the product manager and any necessary contribution to intervention activities will be delivered to support fraud prevention.

POL00423197

3.2.2 Government Services

3.2.2.1 Post Office Card Account (POCA)

Modus Operandi: The use of duplicate transactions through Horizon to target vulnerable POCA customers' accounts, withdrawing amounts of money without the knowledge of the customer.

Programme: Analysis of branch activity through a tracker, mapping trends in transaction patterns as well providing targets for further intervention. A small pilot was instigated at five of the worst offending branches. Following on from this, Network support targeted a further 29 branches using the same script as that used for the initial 5.

Result: The analysis covered an 8 week period and proved useful in identifying branches for intervention. It highlighted one Investigation case, 34 direct interventions with further communications through product streams. The data available were time consuming and resource hungry to collate, making regular reporting unsustainable. Therefore, data relating to only those branches targeted (34 in total) have been considered. There has been a significant reduction in levels of duplicate transactions across this sample of 65%. A new reporting methodology is being developed, which is quicker and easier, to drive better performance management. The Security Team is represented at the POCA risk steering group, who meet quarterly with HP and JP Morgan as well as the POCA decision board who meet periodically to discuss specific cases and agree liability. The "new" POCA2 product has gone through a number of iterations and the Information Security controls have been agreed by the government departments, together with the scope of any accreditation requirements.

3.2.2.2 Green Giro-cheques (HMRC/DWP)

Modus Operandi: Fictitious or over-claims and re-introduction of suppressed cheques. Offices are targeted by external criminals presenting high-quality DWP counterfeit cheques.

Commentary: The business currently is not charged for missing cheques provided that evidence of the transactions can be supplied to the Alliance and Leicester. This does not prevent fraud but providing transactional evidence is sent to the Alliance and Leicester the missing claim is allowed.

POL00423197

In Confidence

Programme / Mitigating Actions: An ACL programme has been developed, which summarises both the volume and value of missing green giros. P&BA are now tackling the worst performing offices by both volume and value to raise conformance levels and identify potential fraud for escalation to Security. Transaction corrections are issued to offices who cannot supply the necessary transactional evidence to support incidents of missing green giros. Engagement is currently taking place with the Business Efficiency Team, who have completed a review on the whole end-to-end process.

All offices have been issued with UV lamps to detect counterfeits and the cheques have been redesigned with enhanced security features.

A new-style DWP cheque with new security features including a colour shifting ink (CSI) design to mitigate fraud was introduced earlier in the year. Despite problems resulting in a large number of impounded cheques and poor customer experience due to cheques reacting to differing lighting conditions, the new design is proving successful.

POL00423197

3.2.2.3 Simple Money Transmission Services (SMoTS)

Modus Operandi: SMoTS is aimed at simplifying a number of payment vehicles to improve compliance, reduce fraud and deliver cost-effective payment solutions. One current project is the replacement of the DWP Green Girocheque with a smart token.

Mitigation/Commentary: The Security Team have provided risk assessments and advice to the SMoTS project team to support the bid for the encashment process, which will continue into 2011.

3.2.2.4 DVLA

Security Objective: To deliver a reduction in levels of manual, reversal and able-to-disable transactions and build a fraud risk management relationship with the DVLA.

Six DVLA fraud cases have been raised for the year, 3 where 'spoilt' or reversed transaction discs were found being used and 3 where vehicles had been taxed without correct documentation

Programme: Monthly data tracker supports early analysis of manual and reversal transactions. Meetings with DVLA identified a common approach to managing fraud risks.

A letter went out to all MVL branches identifying our analysis, concerns and next steps, followed by further monthly phone calls that have identified additional problems with DVLA records and V11 reminder barcodes not working. A "top tips" guide has been produced between Post Office Ltd and DVLA which is being prepared for deployment, with the aim of driving up conformance and maintaining the programme's impetus.

Result: This letter had a significant impact on reversals, reducing by 22% in following two months and has remained constant since then, whilst reduction in manual transactions was 16%. Security will be involved in a business-wide workshop looking at the whole transaction pipeline to improve compliance. The relationship with the DVLA has improved significantly over the last 12 months.

3.2.2.5 Application, Enrolment & Identity (AEI)

AEI services have developed a solution whereby DVLA and UKBA transactions can be conducted through Post Office Branches. The current kiosks, or booths, are being piloted at 17 branches. To allow Post Office Ltd to bid for future business, the success

POL00423197

of the pilot is critical to the 2011-16 strategy. In addition, a new front line service is being developed for passport services, as this is an on-line application process and to meet the needs of customers without access, a solution is required.
Mitigation/Commentary: The booths are currently performing transactions at pilot branches and early signs are positive. Risks raised by franchise partners have been managed along with some physical positioning of equipment in certain branches. The system' s accreditation was achieved in a remarkably short time considering the complexity and nature of the information being captured. A modular approach to the design and documentation has been adopted which places the service in a very good position for further deployment without the need for extensive re-work or full re-accreditation. The front line service will involve staff assisting applications for passports via a laptop, to then allow the biometric information to be completed in the AEI booth. Security has provided support to both elements to ensure we have a holistic solution that supports the business aspirations.

3.2.2.6 Immigration & Passport Service (IPS)
With the "check and send" contract coming to an end, the Immigration and Passport Service have sought tender responses for the capture of biographic and biometric data from UK citizens for the renewal of passports and new applications. Responses have been prepared and submitted and Post Office Ltd has been selected for the next phase of the process. The tender documents submitted drew on the experiences of the AEI project and sought to leverage that infrastructure.

3.2.3 Mails & Retail

3.2.3.1 Rejected Postage Labels

Period	1	2	3	4	5	6	7	8	9	10	11	12
Predicted fraud level 09 / 10	£34,360	£31,072	£31,254	£36,302	£30,764	£28,700	£33,719	£43,874	£83,059	£29,797	£30,142	£23,589
Cumulative predicted fraud level 09 / 10	£34,360	£65,432	£96,686	£132,988	£163,752	£192,452	£226,171	£270,045	£353,104	£382,901	£413,043	£436,632
Cumulative predicted fraud forecast 09 / 10	£34,360	£68,720	£103,080	£137,440	£171,800	£206,160	£240,520	£274,880	£309,240	£343,600	£377,960	£412,320
Number of offices above tolerance	160	179	179	170	187	190	177	274	504	167	192	146

POL00423197

Modus Operandi: Theft of Royal Mail revenue when an allegedly rejected (unusable label is used) and payment from customer is stolen.
Results: At period 1 this year the predicted fraud level stood at £34,360 reducing to £23,589 in period 12.The number of branches above the tolerance level was at its lowest number of 146 at period 12 with only 1 branch being over £500 above tolerance. Although the 12 month predicted fraud level is higher than the forecast fraud level, this is due to the significant spike in December in the number of branches showing between £100 and £200 above tolerance.
Programme / Mitigating Actions: A complete review of the analysis and forecast fraud levels took place at the start of the financial year. This took into account the volume and value of mail transactions going through the branch each month against the volume and value of rejections. Analysis shows the branches above tolerance each month and the top 20 to 30 offices receive a phone call to question their levels of rejections. The branches receiving phone calls have realised reductions of £22,000.
2010 / 2011 Proposals: Phone calls to become a business as usual activity at P&BA. Fraud forecast for December to be reassessed in light of the significant spike in predicted fraud.

POL00423197

3.2.3.2 Spoilt Postage Labels

Period	1	2	3	4	5	6	7	8	9	10	11	12
Predicted fraud level 09/10	£35,767	£29,499	£35,803	£37,083	£38,053	£45,697	£55,078	£41,023	£46,807	£28,490	£27,910	£25,790
Cumulative predicted fraud 09/10	£35,767	£65,266	£101,069	£138,152	£176,205	£221,902	£276,980	£318,003	£364,810	£393,300	£421,210	£447,000
Cumulative fraud forecast 09/10	£35,767	£71,534	£107,301	£143,068	£178,835	£214,602	£250,369	£286,136	£321,903	£357,670	£393,437	£429,204
Number of offices above tolerance	134	173	175	164	188	194	173	220	291	132	161	162

Modus Operandi: Theft of Royal Mail revenue when an amount is entered onto Horizon as spoilt postage but there is no spoilt label present at the office and the amount in cash stolen from the till.
Results: At period 1 this year the predicted fraud level stood at £35,767 reducing to £25,790 in period 12. Although the 12 month predicted fraud level is higher than the forecast fraud level, this is due to the programme not starting until period 7.
Programme / Mitigating Actions: Analysis and forecast fraud levels took into account the volume and value of mail transactions going through the branch each month against the volume and value of spoilt postage. Analysis shows the branches above tolerance each month and the top 20 to 30 branches receive a phone call to question their levels of spoilt postage. The branches receiving phone calls have realised reductions of £29,000. Transaction corrections totalling £41,000 relating to cases raised and non-conformance have been issued this year. The Security Team have worked closely with Business Efficiency to review operational processes and issue the changes to the network via an operational focus article in January 2010. There have been 4 cases raised in relation to spoilt postage this year totalling £34,102.
2010 / 2011 Proposals: Phone calls to become a business as usual activity at P&BA. Transaction corrections to be issued when branches cannot provide the spoilt labels to match their claims. Spoilt postage labels to be checked at routine audits. Explore spoilt postage becoming a supervisor-only transaction. Investigate the potential impact of Post & Go machines on spoilage levels.

3.2.3.3 Mails Integrity

The Mails integrity programme set out to return 313 branches to MI Compliance. After branch surveys were carried out this was reduced to approx 115 branches. Budget of £50k was spent on physical secure storage solutions that covered approx 100

POL00423197

branches. These have been rolled out to approx 40 branches so far, with roll-out to be completed in 10/11. business as usual and HNGx survey processes for emerging non compliant branches has been completed.

POL00423197

3.2.4 Telecoms

3.2.4.1 Telephony Bad Debt

The bad debt on our telephone service is part of an Industry-wide concern, with 4% to 10% of all customer accounts in debt, whilst Post Office Ltd currently has around 6%. To date, over £13m has been placed with a third party for recovery. This is an ever-changing figure since, as debt is repaid, new debt emerges.

Mitigation/Commentary: The scale of the problem in identifying the "can't" pay and "won't" pay has led to the business employing the services of a third party (Roxburgh) to manage the control of this debt. This is an Industry standard practice. There are a suite of activities that are used from basic call collecting from call centre staff to newer technologies, such as call barring, account tagging as well as direct visits to customers. Targets are set by Post Office Ltd under an SLA to increase the potential to recover. This year, Roxburgh have recovered £2.8m, with Post Office Ltd writing off £3.8m. Next year, tougher targets (£150K per week from £75K) are to be set along with other technologies and Business Efficiency programmes to increase Post Office Ltd's capability to reduce telephony debt.

3.2.4.2 Phonecards

The 3-D Secure facility, that transfers liability to the banks for purchases on the website, was temporarily unavailable for a short period and during this time Post Office Ltd lost approximately £2k through fraudulent transactions made from the United States.

Mitigation/Commentary: A decision was quickly made to temporarily remove this transaction from the website until the situation with 3-D Secure was resolved. Once resolved the product was re-instated on the website and agreements were made with Royal Mail for a new communication process to notify key stakeholders of any issues relating to web-based purchases.

3.2.4.3 E-Top Ups

Post Office Ltd had an outstanding liability of £67k for refunded E-Top Ups over a 4 year period a review of the product was conducted but contractual requirements from the service providers prohibited any change.

POL00423197

Mitigation/Commentary: The outstanding liability was written off against the product and any new recharges will be charged back to the network through transaction corrections, as agreed between Security, the product manager and P&BA.

POL00423197

4. Information Security Risks & Business Projects

4.1 Invitations To Tender (ITT)

4.1.1 Merchant Acquirer ITT

The current Post Office Ltd contract is with RBS Worldpay (RBSW, formerly Streamline). Under this contract, RBSW acquire all debit and credit card transactions that have been undertaken in our branch network, internet sites and in its call centres including those outsourced to third parties or via joint ventures. RBSW currently process 45m transactions per year at a net annual cost of approximately £4.5m.
Commentary: The Security Team are now working with the Acquirer ITT team to ensure robust fraud control and reporting performance measures at a lower cost are put in place to realise savings (circa £500k p.a. reduction in costs).

4.1.2 Pre-Paid Debit Card ITT

Post Office Ltd is looking to launch a Post Office branded Prepaid Card, for use as a general sterling spend card. There is no equivalent general spend Post Office Ltd product, although the card will function in a similar way to our TMC.
Commentary: The Security Team is working with the product team on a proposal to identify appropriate supplier(s) that enable us to procure a solution.

4.1.3 Cheque ITT

Modus Operandi: Post Office Ltd decided to continue to accept cheques as a Method of Payment (MOP), requiring a new contract as the existing contract for cheque processing was coming to an end.
Commentary: The Security Team reviewed the ITT documents for each bidder and provided the Cheque ITT board with individual scores. It has been announced that the preferred bidder for the cheques contract between 2011 and 2016 is Barclays Bank plc, underlining our commitment to continue accepting cheques as a method of payment. Barclays have required the provision of considerable amounts of information regarding the security of Post Office Ltd systems. In addition assurance on the levels of security being applied, policies in place and rights of audit need to be discussed.

POL00423197

4.2 Connect 2010

Issue/Risk: Royal Mail Group is replacing the current IBM/Lotus Notes Collaborative working environment with a hosted service from Microsoft. The business case has been made on the basis of minimal security components over and above the basic offering and consequently the solution is unlikely to meet Post Office Ltd' s requirements.

Impact: Post Office Ltd may be in breach of regulatory requirements by failing to maintain adequate records of communications through logging systems leading to fines and loss of business credibility. Should user be permitted uncontrolled access to systems from web-based devices, there is a considerable risk that sensitive business information could be compromised.

Mitigation: The submissions by the service providers (CSC and Microsoft) have been evaluated to identify where adjustments might need to be made to arrive at a suitable compromise between functionality and security. At the time of writing the web functionality has not been enabled as the risk of doing so is currently seen as unacceptable.

4.3 Web re-platform

Issue/Risk: The current Royal Mail Group web platform upon which Post Office Ltd' s services are provided is to be replaced in 2010. The Security Team worked closely with Royal Mail Group throughout the tendering and evaluation and a supplier, Cap Gemini, has been identified. The evaluation was based on a number of factors, and whilst this supplier may not have been the optimum from a security perspective, their submission was considered acceptable. There are a number of concerns around the re-platform which it is proposed will make use of "cloud" computing, which has a security model based upon being able to protect the application and data without relying on the protection of the infrastructure.

Impact: Since it is not possible to say with any degree of certainty where the data or application is housed, this will be a challenge for Post Office Ltd' s Government and Financial Services clients as no "cloud" based system has yet been formally accredited.

Mitigation: Engagement with Royal Mail Group is underway and Post Office Ltd' s requirements are being included, with an acceptance from RMG that there may be a

POL00423197

requirement for a more stringently controlled environment and the specification for this, together with the outcomes of security testing, will involve consultation with Post Office Ltd.

4.4 Bank of Ireland (BOI) / Post Office Financial Services (POFS) Governance
Issue/Risk: Following the suspension of the Globe programme, clarity on roles and responsibilities from BOI has been less than forthcoming. It is often the case that products are supplied from the end of a long chain of sub-contractors separated from Post Office Ltd by POFTS, BOI, a 3rd party to BOI and sometimes further. Where issues arise, their resolution and the agreement of standards are matters that require more clarity.
Impact: Unresolved issues that are identified in the BOI systems through the vulnerability scanning process may result in damage to Post Office Ltd' s trading position and brand reputation. A lack of visibility of Information Security Management across the relationship with BOI may result in the inability to resolve issues or identify potential weaknesses in the systems or processes.
Mitigation: During the year additional focus has been placed on this area and BOI have responded positively. Progress is being made in the areas of vulnerability management and secure communications, which it is fully anticipated will lead to wider future benefits. As a side-effect of the work being done in the Security Team, Service Delivery is able to leverage the contacts and issues being identified.

4.5 Horizon Online
Issue/Risk: The migration to Horizon Online is a major change to systems and to the processes followed by both Post Office Ltd and Fujitsu. Delays in the programme and changes to the Fujitsu management structure have led to issues affecting the ability to sign off the service as "secure" and meeting acceptance criteria.
Part of this migration will see the vast majority of branches subject to a physical verification of cash and the Security Team have factored in the potential impact of fraud cases.
Impact: Failure to establish a secure system will impact on the ability to assure our key clients that their information and transactions are safe. In addition, it will not be

POL00423197

possible to establish the appropriate regulatory requirements have been met. Failure to meet the acceptance criteria will result in further delays to the programme.
Current figures, based on branches that have already migrated, suggest that the volume of cash shortages can be dealt with by the Security Team. Should the volume of cash shortages increase, there are back-up plans to deal with these.
Mitigation: There is now a programme in place to deliver ISO27001 certification for the whole environment (including POL-SAP and Credence) and to resolve outstanding "High" Acceptance Incidents for Horizon Online, addressing the governance of the service. Fujitsu are working to meet the security acceptance criteria and address Post Office Ltd concerns about risks to the programme and Security have identified a number of SLA/OLA requirements for consideration by Service Delivery.
Engagement continues with stakeholders, primarily the Horizon Team, Network Support and P&BA, through various channels, including the Fraud Forum. As migration rate increases, it is anticipated that weekly conference calls will be held to check losses, deal with as agreed and highlight branches of concern pre/during/post migration.

4.6 Counter Transactions
Issue/Risk: Controls at the counter, to ensure the correct processes are followed and clerks are required to verify the amount of keyed transactions, are not fully in place.
Impact: The scope of error, especially with "free-keyed" transactions, is increased and it is not possible to always enforce business rules.
Mitigation: This is largely an issue with transaction design and will require engagement with the owners of the individual transactions concerned, together with Network and Suppliers.

4.7 Use of flexible technologies
Issue/Risk: The lack of direction on the use of flexible technologies and constant reinvention of solutions to common problems leads to the presence of a large number of bespoke solutions requiring maintenance. The development of a unified approach is hindered by the lack of resource for infrastructure development.
Impact: In addition to the cost implications, a fragmented security model is more complex and difficult to maintain, resulting in a less secure environment overall.

POL00423197

Mitigation: Work has continued with the Strategy and Architecture group to ensure developments continue to use security components that are re-usable and sufficiently flexible to enable good deployment of security without the use of multiple bespoke technologies or reduction in agreed control processes. As an example, although Active Directory may not be a universal directory of choice, the use of it in authenticating users removes the need for multiple platforms and multiple userIDs.

4.8 Non-approved implementations

Issue/Risk: This continues to be a problem with the availability of externally hosted systems to which business units are able to connect and engage. There have been instances where hosting of material has been passed to external agencies without the project passing through the Change & IS gating process and consequently being considered for information security.

Impact: This is especially a risk for the integrity of the information being provided to the Public, where defacement would be highly embarrassing.

Mitigation: Where these are identified a degree of fast-tracking through the appropriate processes has been undertaken in conjunction with the supplier to ensure any issues are addressed. Relationships with business partners and analysts are being improved and are already resulting in earlier and better engagement.

4.9 Government Security Policy Framework (SPF)

Issue/Risk: The submission to Cabinet Office is once again being prepared in conjunction with RMG. On the whole there is general agreement on the level of compliance with the specified controls, although in some areas Post Office Ltd still needs to submit a separate response. The result is that the reported compliance from Post Office Ltd will be either "Full" or "Not Applicable" which reflects the differing nature of our businesses and attitude to risk.

Impact: Failure to present a unified and constant approach may lead to confusion with Government Clients as to the compliance status of Post Office Ltd. Any confusion in the area, will result in greater scrutiny from clients and loss of confidence.

POL00423197

Mitigation: Adherence to the SPF has been material in discussions with Government Departments (and some other clients) for the provision of assurance on the controls Post Office Ltd has in place around our IT systems, Information and Governance. An approach has been agreed with Royal Mail Group and a thorough review of the policy framework is now underway.

4.10 Infrastructure

Issue/Risk: There is considerable reliance upon centrally provided infrastructure components to secure Post Office Ltd' s day-to-day business, although the threat has changed faster than the infrastructure model. Increasing coverage in the media of data compromises has made a number of clients more cautious and regulatory bodies more vigilant.

Impact: Users with the ability to move information through insecure means (such as USB devices and CDs) expose the business to risk of compromise of that data. The sending of sensitive information via email is akin to writing it on a postcard, although this does not appear to be appreciated by the user community.

Mitigation: Projects have delivered a secure ad-hoc file transfer system, doing away with the need to send sensitive documents via eMail using proprietary products such as PGP. All client PCs are now protected with a firewall which can be configured to prevent external attacks when not attached to the Post Office Ltd infrastructure and the roll-out of protection for files saved to external devices is underway. Other projects have examined the use of "Data Leakage Prevention" technologies together with mitigation of the risks associated with the availability of local administrator rights on client PCs and these will form the focus of activities next year.

POL00423197

5. Emerging Risks, Threats and Initatives2010/11

5.1 Business Losses Programme

The business loss target 10% reduction led by Business Efficiency will be supported by the Security Team in 2010-11, expanding the focus from losses due to crime to all losses.

5.2 Fraud Management Information, Intelligence and Lessons Learnt Programme

Security objective: To develop the casework failures reporting to provide lessons learnt initiatives for future programme activity and draw all relevant Intelligence streams into coherence reporting for analysis.

Programme: The current failures database was assessed to consider its viability to support the objectives of this programme. Data captured was inconsistent, patchy in quality and relied on subjective interpretation. Ideas centred around an on-line application, which fed into a single database where this information, along with other processes currently fed in manually, could be captured. The significance of this change would impact on the whole casework data capture and management process and could not be progressed in isolation.

Result: As this potential approach needs to be viewed alongside the other processes for re-coding internal crime data, the findings and requirements are being considered within the wider casework piece, and this would form one part of a more intelligence-based system that provided crime management data for analysis.

5.3 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 (PID) has now been produced and approved, with a Programme Plan setting out key milestones in preparation for launch.

5.4 Information Security Impact and Risk Assessments

POL00423197

The process for the completion of Security Impact Analysis, which is essential in understanding the impact of systems and products, has been passed to the Solutions Architects where it is resulting in earlier engagements and consideration, although there is still a considerable amount of coaching required.

The recent review by Comsec consultants is expected to result in a revision to the methodology and reporting of risk analysis. Key risks identified were counter transaction process security controls, limited SLAs within information security area and lack of resources for monitoring security recommendations. Their proposed next steps are to agree risk tools and processes, review outstanding risks and develop mitigation plans (or Risk Acceptance Notices) for them.

POL00423197

5.5 Malicious Web Activity

Post Office Ltd systems recorded a number of the "scanning" type of attack through activity monitored at the network perimeter, but no evidence of any targeted activity. The nature of such probes is that they identify weaknesses in the security controls and then seek to exploit them. The vulnerability management systems in place are designed to identify and control such weaknesses and it is imperative they continue to be supported.

5.6 Phishing and Spam

This type of attack has continued over the past year, despite falling in popularity since the peak in 2007/2008. In the Post Office Ltd environment, the majority of such attacks are trapped at the eMail gateway, although some do continue to reach end users. Where users are persuaded to follow a malicious link, so far all such traffic appears to have been stopped through either the "Websense" filters, or at the Internet proxy servers.

The biggest risk to Post Office Ltd infrastructure here is through users connecting through home or other uncontrolled access points where these measures are not in place. Configuration of client firewalls to ensure more stringent rules are in place for non-Post Office Ltd infrastructure will mitigate against such risks.

Royal Mail has recently been used as a vehicle for mounting attacks, although only by the use of eMail communications which purport to originate from RM. So far there is no evidence that Post Office Ltd' s brand has been similarly abused although this status continues to be monitored through Internet alerting facilities.

5.7 Information Security Targeted Attacks

The highest proportion of targeted attacks has been against the opportunity for identity theft and misappropriation of payment details, including payment cards. On the whole these have been against individuals through the use of malicious code or websites and via phishing activities. Attacks against companies have tended to be either through the use of insiders or through insecure wireless networks. Post Office Ltd have in place employment policies to mitigate against the former and wireless standards for the latter. Where risks persist is in the connection of unauthorised

POL00423197

equipment and we have been working with suppliers on processes and technologies for detecting these.