POL00423218

Post Office Ltd – Security Process

GRAPEVINE INTERNAL FRAUD REPORTING PROCESS

Document Information

Title	Grapevine Internal Fraud Reporting Process
Category	Process document
Subject	Security
Version Control	Version 2.0
Author	Wayne Griffiths
Owner	Head of Security, Post Office Ltd
Enquiries	Wayne Griffiths Security Programme Manager Mobile GRO Mobex GRO
Purpose	To define the process on the handling internal fraud/security breaches through to Grapevine
Audience	Post Office Ltd Security Team, Post Office Ltd Management, Grapevine call handlers, key identified internal stakeholders.
Keywords	Grapevine Internal Fraud Reporting
Privacy level	Post Office Ltd Management
Document format	Chevin Light 12
Document type	Electronic (MS Word. Document), Paper,
Review date	Annual
Expiry date	Ongoing subject to review

APPROVAL

Role	Name(s)	Date
Business input	Security – Commercial Strand	June 2011
Assurance	John Scott, Head of Security Post Office Ltd	
Authorised	Head of Security, PO Ltd	

Version control

Version No.	Reason for issue	Date
Version 1.0	New Process (separation of process from Policy)	Sept 2011
Version 2.0	Amendments to embedded process map	Oct 2011

POL00423218

Introduction

The Grapevine intelligence service will extend its product portfolio to include handling and progressing incoming calls based upon internal fraud or breaches of security procedure at Post Office Ltd (POL) locations, primarily in relation to Network and Supply Chain sites.

Whilst it will not necessarily be possible to substantiate individual claims made, these calls will act as a trigger mechanism for the Crime Risk Strand to commence further analysis of that site, which may indicate a more serious problem. Potential fraud issues may then require intervention activity, whilst security breaches may require a visit by a Security Manager. It is of paramount importance that the callers identity remains anonymous, and the reason given for any such visits or calls should be purely ad hoc, rather than as a result of specific information received.

The Public Interest Disclosure Act (PIDA) of 1998 states that the disclosing of confidential information such as illegal activity or environmental breaches should not result in reprisals, recriminations or retribution against the information provider. Even though the Internal Fraud Reporting Service isn't an official Business 'Whistleblowing' facility, calls received should be handled confidentially and professionally to ensure there is no negative come back on the information provider.

Under normal circumstances, the observer of fraud or security breaches should report them through their line management structure, however, they may feel unable to do this for fear of reprisal or recrimination. It is for this reason that the Grapevine Internal fraud Service is being introduced.

Policy/Process documents

This process document maps out in detail how incoming calls should be handled by the Grapevine service provider, It also goes on to explain how calls should be

POL00423218

escalated back into the POL Security Team for further investigation.

This document also makes reference to the process involved in dealing with calls received which may be more appropriate or applicable to other Helpline service providers within the Royal Mail Group.

The process should be read in conjunction with the Grapevine Internal Fraud Policy document which explains the rationale behind the service provision. The policy document is embedded below for reference.


C:\Documents and Settings\wayne.griffi

Initial Call Handling

Incoming calls will be made to the generic Grapevine helpline number GRO. It is imperative that the call is handled discreetly and professionally as the caller may be under stress, and unsure they are pursuing the correct route.

The operator should be at pains to make the caller feel as comfortable as possible, and should be reassuring them that they have made the correct decision in making the call.

It is anticipated that calls received will fall into 2 main categories, these are:-

- **To report colleague malpractice.** That is to say for example, that Clerk A observes Clerk B taking cash from a Post Office till, but feels uncomfortable in reporting it through the line management process.
- **Repeated security breaches within the workplace.** For example, a safe being continually left ajar, especially if in public view. Again, the caller feels unable to report through normal line management channels.

The call handler should record as much information as possible on the form embedded below. They should also be aware that the caller should be allowed to talk, and

POL00423218

divulge as much information as possible, as they may not have further opportunities, or the inclination, to do so.


C:\Documents and Settings\wayne.griffi

Dealing with Calls not appropriate to Internal Fraud

It is entirely feasible that calls will be received on this helpline that are of a different subject or nature to the intended usage. Under these circumstances, the call details should still be taken, with the proviso that the caller should be informed that the information will be passed on to the appropriate helpline or service.

It may be prudent at the outset of such a call to advise the caller that they may wish to call the appropriate service themselves (relevant number below should be provided), which would allow them to engage with a more suitable and knowledgeable call handler. However, if the caller declines this offer, comprehensive details must be taken and passed onto the most appropriate service.

It is anticipated that calls through to the Grapevine Helpline in error would fall under the categories stated below, along with the correct recipient service provider details.

- **Bullying & Harassment Helpline** GRO can only give advice, incident reporting should be made through the HR service.
- **HR Help** GRO GRO GRO for reporting issues of a personal nature
- **Corporate & Social Responsibility Helpdesk** GRO GRO) for reporting issues with an environmental impact.
- **Corporate Security Helpdesk** GRO GRO) for reporting any RM security issues
- **Speak Up Line** (GRO GRO for reporting any other RM related calls

Calls therefore received and documented which are more appropriate to one of the services listed above should be re-routed as applicable.

POL00423218

The embedded document below maps and demonstrates this process.


C:\Documents and Settings\wayne.griffi

Information Escalation Process

When a call is received that is pertinent to this service, an information capture sheet must be completed in as comprehensive a manner as possible. The caller may or may not volunteer their name, however, whilst they must be informed that the content of the call will be investigated, they should also be advised that there will be no direct feedback given on findings.

It should be noted that any call subsequently found to be of a malicious nature, the disciplinary code may be invoked against the perpetrator of the call if their identity is known.

Once all relevant information has been gathered, the form should be e mailed to PostOfficeSecurity GRO with **'Internal Fraud Reporting'** displayed as the text in the subject box.

Security Internal Escalation Process

Once received by the POL Crime Risk Admin Team, this should be escalated to a Manager within the Strand. The information received within the e mail, if in relation to suspected fraudulent activity (that is to say impacting on products or cash as a result of internal fraudulent actions), should act as a trigger for further analytical work to be undertaken by a Crime Risk Analyst to profile the office in question. It may be that this will throw up potential irregularities that may need some intervention activity. Under these circumstances, liaison should be undertaken with the most relevant partner/stakeholder (Audit Team, or Operations Strand possibly), to appraise them of the situation, the findings, and to agree on further actions. It must be stressed however, that the original complaint is not necessarily being investigated, it is this information which is used as a trigger to undertake further analysis of the office in question.

POL00423218

Likewise, if the initial call relates to physical security breaches at a location (safe or access door left open for example), the information should be shared with the Operations Strand by e mailing the relevant Team Leader, and a 'Torch' type visit by a Security Manager may be the most appropriate method of follow up.

As stated earlier, any intervention activity undertaken as a result of the original information should be under the guise of business as usual. That is to say, part of security activity within the general area. Under no circumstances should it be divulged that the visit is as a direct consequence of information received from an internal source.

Although this service isn't a bona fide 'Whistleblower' line, callers are still covered by the 'Public Interest Disclosure Act 1998' (PIDA). Therefore there can be no reprisals or recriminations against the person making the allegation (unless malicious). Anonymity is a key driver, and it is worth repeating that any resulting security activity must be dressed up under the 'business as usual' banner, and not reported as being as a result of specific information received (by an employee).

Any genuine calls that are received but, after analysis, do not lead to more substantial concerns, should be filed securely by the Casework Team in case any action is required at that location in the future.

The embedded document below maps this process.

C:\Documents and Settings\wayne.griffi