POL00030670

IS05
Conduct of Criminal Investigations Policy

Document Control

1 Overview

Owner:	Head of Security Operations	Enquiry point:	Head of Security Operations
Version:	0.2	Effective from:	29th August 2013
Last updated:		Last review date:	
Review period:	Annually or major change		

2 Revision History

Version	Date	Author	Changes
0.1	16/08/2013	Rob King Andrew Wise	Initial draft.
0.2	29/08/2013	Rob King Andrew Wise	Update post Senior Stakeholder Review.

POL00030670

1 Purpose and Statement

Properly conducted investigations form a key part in our strategy in protecting assets and reducing loss. If poorly managed, an investigation can lead to increased risk of future loss and significant damage to the corporate brand. In commencing any investigation we need to consider the impact in terms of the protection of business assets and limiting potential liabilities weighing against the reputation of the organisation or damage to the brand should the investigation fail. Post Office Security is almost unique in that unlike other commercial organisations we are a non-police prosecuting agency and are therefore subjected to the Codes of Practice and statutory requirements of the Police and Criminal Evidence Act.

There is another anomaly that sets us aside from other commercial investigators. Of our 11,800 branches, only 370 are currently staffed by employees of the Post Office. In the majority of cases branches are either Franchisees or Agents that receive remuneration. As neither is deemed to be employees of the Post Office, the usual practices and procedures of an employer employee investigation do not apply.

In cases where fraud is uncovered and good evidence of criminality exists, then a criminal investigation will invariably commence. At the same time Post Office Contract Advisors have the responsibility to ensure that any contractual breaches are investigated and impact on the business is minimised. As a result close communication needs to be maintained between the Security Manager investigating the criminal investigation and the Contract Advisor who needs to maintain Post Office services. If this relationship is robust then sound decisions can be made with the benefit of all the facts and evidence shared to ensure that there is a successful outcome to the investigation that benefits the business.

With the stakes so high, the department must be seen, internally as well as externally, to be acting fairly, appropriately and within the law. The investigation needs to be properly conducted to establish evidence that will support a successful criminal prosecution.

2 Goals

This guide been prepared as part of the case file review and is intended to support Security Managers from the commencement through to the conclusion of the investigation. Included in the document is comprehensive guidance of the

POL00030670

process including key points to consider at various stages of the investigation.

Prior to commencing an investigation the Security Manager will have to consider

- The Seriousness of the allegation
- The level of criminality
- Any contractual, compliance or regulatory concerns
- The potential to damage the reputation of the Post Office
- The expectations of key stakeholders

3 Scope

The scope shall include the operational services, operations, external communication, information sharing and platforms, services used to support the Post Office including those hosted and managed by suppliers and partners.

4 Policy Statement

CASE RAISED

Cases are raised from various sources, in each instance the information is passed to the relevant operational Team Leader who will evaluate the allegation and decide whether or not a case should be raised.

A shortage at audit will result in the completion of an Event Capture Form (ECF) report by the lead auditor. The ECF report is then emailed thorough to the Post Office Security Casework Team. On receipt of the ECF (where a suspension has taken place), this is passed onto the relevant Team Leader who will make the decision whether to raise a case or not. If this is an immediate open enquiry the case will be raised before the ECF is received.

All losses where a suspension has taken place are raised this way, although the loss is not always due to criminal activity. The Team Leader should review the circumstances surrounding the audit shortage and assess whether an investigation is the most suitable course of action.

The following are examples of types of audit shortages.

- Cash Shortage at Audit No Explanation
- Cash Shortage at Audit Comments made at audit
- Cash Shortage - member of staff (Not the SPMR) suspected of criminality
- Cash Shortage - Loss hidden Transfers

POL00030670

- Cash Shortage – Loss hidden Remittances
- Cash Shortage – Loss hidden Giro Suppression
- Personal Cheque in Drawer
- Cash Shortage in ATM
- Cash Shortage in Lottery

Post Office Card Account (POCA) cases; On occasion, the Hewlett Packard (HP) Call Centre is contacted by customers who claim they are victims of fraud. The Post Office Card Account Primary Account Holder (PAH) may identify persons who they suspect have defrauded them and on occasions they are staff or Agents of the Post Office. The PAH allegation will be received through the HP Call Centre who, working on behalf of Post Office Ltd, manage the day-to-day POCA service. HP operators are requested to record as much detail as possible and report the allegation to Post Office Ltd Security, Details of the complaint will be passed onto the Team Leader. On receipt, the Team Leader should make an assessment on the validity of the claim. Should they find no reasonable grounds to support the claim they should return it to the Admin and Support Team within 5 working days with 'NO CONCERN' annotated in the Security Comment box. In the event the case is worthy of further investigation they are to request a case number and pass to their Team for investigation.

Cases can be raised in relation to a specific client; these can come from various sources such as direct from the client via the Commercial Security Team, a complaint from a customer or analysis from the Grapevine Team. In each case the request is emailed to the Team Leader to review the details and assess whether an investigation should take place. Post Office Ltd has a massive client base; the following are examples of some of the more usual cases to be raised.

- DVLA
- Royal Mail
- DWP
- Government Services
- AEI Machine

Cases also can be raised from various other sources.

- Crown Office Issues / Loss
- Suspicious Transactions
- Remuneration
- Contracts Manager
- Police Request

These types of enquiries are sent to the relevant Team Leader who will make the decision whether to raise a case or not. The Team Leader informs the Casework Team via email

POL00030670

that a case is to be raised and which Security Manager will be dealing with the case.

The Casework team then complete the new case raised document and email this to the security manager along with any ECF or audit reports which they have received.

The stakeholder Notification forms part of the New Case Raised Document. Within this document details of all stakeholders are listed.

Once a case has been raised the Stakeholder notification should be emailed to all stakeholders, casework team and Team Leader as soon as possible. The investigator should ensure that as much detailed information is included on the stakeholder notification.

Communication with the commercial team is essential. Ensure that all stakeholder updates throughout the investigation are copied to the commercial security team.

A copy of the stakeholder notification should be printed; this is associated in Appendix C of the case file.

EVENT LOG

All activities undertaken during an investigation should be recorded on the event log; this should also include reasons for delay in progression of a case file.

The event log should be printed out and submitted with the green jacket. This should be updated and a new event log entry inserted at each stage of the investigation.

SUPERVISION OF INVESTIGATION

The decided course of action needs to be proportionate and necessary. It may, if the circumstances warrant be more appropriate to consider other actions that could be done that don't necessarily lead to a criminal investigation. Examples include pursuing a civil enquiry for breach of contract, civil debt recovery, training review refresher, briefers, additional auditing, a caution, warning letter and or NFSP engagement. Some of these possible outcomes may not be obviously apparent until the suspect is interviewed, although they should be built into the process at this early stage. Close communication and co-operation with key stakeholders is essential to ensure, proper and considered course of action is taken.

Proper consistent supervision is vital to ensure that cases are thoroughly investigated and submitted in a timely manner. Team leaders with the support of the Financial

POL00030670

Investigators need to quality assure the investigation making sure prior to initial submission that all available evidence has been gathered.

From the point the case is first raised Team Leaders should give due consideration to the merits of a criminal investigation.

INVESTIGATION

It is important to consider the aims, objectives and scope of the investigation. Not all Post Office investigations are criminal; the Security Manager may be called upon to investigate employees under the grievance and disciplinary procedure. It is important to determine what type of investigation is required, what time frames are in place, available resources and what other issues may affect the conduct of the investigation. An example may be a flag case with potential to damage the reputation of the business where senior stakeholders have an on-going interest in the progress of the investigation.

When a case is raised the Security Manager needs to prepare an investigation plan which will outline the terms of reference in the way the investigation will be conducted. Points to consider include:

- Risk assessment
- Duty of care
- The source of the investigation
- Statutory, regulatory or compliance considerations
- Impact on the organisation
- Media
- Timeframes
- Immediate open enquiry

In all cases stakeholder engagement is essential, updates to stakeholders should be sent on a regular basis especially at relevant milestones such as interview, file submission and summons served. For high profile cases such as crown office losses updates should be more frequent and include key senior stakeholders in the relevant directorate.

For cases raised due to audit shortage, communication with the auditor on the day of the loss or as soon after the case is raised is essential to gain an understanding of the loss and to ensure they will send all audit documentation (original documentation) to the investigator.

In all cases where a loss has been identified and a SPMR has been suspended a case conference should be arranged with the contracts manager at the earliest opportunity. This is essential and allows exchange of information and an

POL00030670

understanding the expectations and direction the contract manager is planning in relation to the conduct. Attached below are timescales and expectations for the contract process.

There may be occasions where criminality is suspected that a request is made directly to a contract manager to consider suspending the SPMR. In these circumstances the Security Manager must provide a detailed explanation outlining the rationale supporting the request. A record must be kept of this decision which may at some future stage have to be justified in court proceedings

The Security Manager has been tasked to prove or dispel the allegation. In criminal cases where the burden of proof is beyond all reasonable doubt, it is necessary to draw on all available evidence which is likely to substantiate the allegation. In cases concerning the Horizon system, it is important to establish the level of training the subject received, when this was received and action the subject took to remedy any identified faults. A key points to cover template has been produced to ensure that Security Managers establish these facts during the interview process. As part of the evidence gathering process, the Security Manager can collect evidence from various sources including :

- Statements from witnesses [current, previous members of staff]
- Expert witnesses
- Post Office accounting and HR databases
- Contract Advisor database
- CCTV
- Banking records
- Telephone records
- Interviews with suspects

It is vital that all available witnesses are interviewed. If there is a good reason for not doing so this must be recorded in the progress of investigation log.

The Security Manager must not overlook the fact that a fair investigation is there to establish the truth as well as substantiate the allegation, so it is important that any evidence uncovered that may support the suspect's position is also recovered. It is important to document every action, decision and reason for decisions being made during the course of the investigation.

ENQUIRY TYPE

Immediate Open Enquiry.

- Where immediate response is appropriate and few pre-interview enquiries are needed or practicable.

POL00030670

Major Enquiry
- >£15,000 (or major customer / client / reputation impact) where immediate response is not possible due to the requirement to perform pre-interview enquiries / analysis.

Standard Enquiry
- All other enquiries not included in the above - where immediate response is not possible due to the requirement to perform pre-interview enquiries.

Liaison
- Any case where liaison with another investigative body leading enquiries into criminal activity at Post Office Ltd branches.

INTERVIEW FRAMEWORK AND TIMESCALES

All significant steps in the investigation including any lengthy delays in concluding the enquiry need to be recorded. The progress of investigation document will eventually form part of the unused material and should be produced with the file. The details of investigation need to be sufficiently informative although an element of objectivity needs to be applied.

Significant points can become critical should the enquiry concern non availability of witnesses, external stakeholders or any other influential factors which may force undue delay.

A culture needs to be embedded where Security Managers are aware and fully understand the importance of providing a comprehensive chronological account of an investigation, not merely to avoid undue criticism, but also where there could be an issue with the case at some later stage which may undermine the likelihood of successful prosecution.

Interview Date
- Offender should be contacted and Interview should be arranged without delay. Timescales will depend on preparatory work that needs to take place prior to this. Good Evidence Takes Time. In complex cases there may be a need to conduct a preliminary [holding] interview with a more detailed interview taking place when further enquiries have been completed.

Immediate Open Enquiry
- Interview on day of notification (where possible) minimum within 48 hours and case submitted to normal report timescales (12 days)

Major Enquiry

POL00030670

• Case to be at "suspect offender" interviewed within 1 month of case raised.

Standard Enquiry
• Case to be at "suspect offender" interviewed and submitted / closure stage within 2 months of raise. Should enquiries indicate increased loss or impact, status must be amended to Major Enquiry immediately.

Liaison
• Regular contact should be maintained with the authority (Police, Royal Mail, DWP) dealing with the case.

• After the first month the investigator should discuss the case with their Team Leader and a way forward agreed, this will ensure that the liaison case is progressed.

EVIDENCE

Good communication with the audit team is crucial to ensure evidential resilience in relation to the continuity of exhibits. Every effort must be made to ensure that the person finding is the person exhibiting and original documents that will form the evidential basis of the case are retained until collection. The continuity will be stronger if the documents seized are secured and handed over against a signature. In circumstances where the only viable way is to send the documents through the post they should be sent by the Auditor to the named Security Manager by Special Delivery.

Auditors are to be encouraged to record any significant comment made in the course of the audit either unsolicited or in response to a reasonable question to complete the audit such as "I have checked the money in the safe and there appears to be a shortage, is there any money stored elsewhere that needs to be checked" . In the case of the unsolicited comment, the auditor should record this ie I know you will find a shortage, I borrowed the money. However any further question such as "why" would constitute an interview and the Auditor must refrain from asking such questions.

In such cases, the Auditor should inform the suspect that their comment will be recorded but any further questions concerning the comment may be conducted under caution by a Security Manager where the suspect has been accorded their rights. This should not distract from the role of the auditor and questions around should still be asked to verify financial assets due to Post Office LTD.

In cases where the suspect wishes to make comment, the Auditor again should record the initial comment, advise the

POL00030670

suspect as above and if they continue, note in the record, that the suspect was advised that they would have the opportunity to be interviewed by a Security Manager under caution at a later stage. THEN CONTINUE TO RECORD THE COMMENT. Again any questions even for clarification from the auditor would constitute an interview and could/would render the evidence inadmissible so the Auditor must refrain from asking such questions.

BACKGROUND CHECKS

Local Management Checks

- Contact with the contract manager is essential; they can provide the investigator with a background on the individual along with providing all information relating to the branch from their database.

Training Records

- A request for the branch training history should be made to the Network Support Admin Team email address. This will detail what training was received for the SPMR when he was appointed to the branch, it will also show any intervention training requested or delivered for the branch. It is the SPMR's responsibility to train his staff, no records for training (apart from compliance training) is kept for SPMR assistants.

Post Office Ltd Human Resources Printout. The Sub Postmaster Printout or employee printout should be obtained for all cases by emailing Human Recourses using the HR Assistant Checks email address. This document can provide the following information –

- The subject's personal details, such as NI number, home address, bank account(s), next of kin,
- Date the SPMR was appointed.
- Claims data (i.e. holiday pay) & dates the SPMR was on holiday.
- The full SPMR file can be requested by emailing 'Contract Admin Team'

P356 Assistant List. The P356 Assistant list should be requested at the same time as the HR Printout from the HR Assistants Check email address. This report can provide the following information

- Name, date of birth and NI number
- Persons registered to access Horizon (users), at that Post Office
- The Horizon user's identities for each assistant.
- Whether the assistant is a permanently employed or temporary/holiday relief
- Date the person was activated to use Horizon and the date users were removed from the Horizon system.

POL00030670

SPMR Remuneration. The remuneration from a particular branch can be obtained via an e-mail to HR Agent Remuneration.

Police National Computer (PNC). Post Office Limited PNC checks can be made for intelligence gathering purposes in respect of individuals and vehicles suspected or known to be involved in crime against the Post Office Ltd. Examples of authorised use are as follows:

- To assist authorised personnel with intelligence gathering around individuals suspected/ known to be involved in committing criminal offences.
- For operational Health & Safety considerations and evaluations prior to suspect offender engagement as part of the operational risk assessment.
- To obtain previous conviction details of defendants and witnesses for cases being prosecuted by Post Office Ltd.
- To establish intelligence with regards to vehicles and occupants suspected to be involved in criminal activity against the Post Office.
- To identify the registered keeper of vehicles connected to the address of a suspect/known offender involved in criminal offences against the Post Office Ltd.

Do not conduct checks for the following reasons:

- Unsubstantiated allegations about an individual.
- “Fishing trips”, for example blanket checking vehicles or persons such as all vehicles in a staff car park in an effort to identify a suspect’s vehicle.
- To identify ownership of a vehicle in accordance with Proceeds of Crime Act.

Equifax investigators can rely on Equifax to provide the following information:

- Personal details
- Addresses
- Court and Insolvency Information, (i.e. county court judgments)
- Alert Indicators (Office of Foreign Assets Control)
- Alias and all names used
- Associates
- Electoral data confirmation
- Credit transactional activity, including the client and transactional history
- Record of searches done by Equifax clients, (i.e. banks and retailers)
- Property valuation
- Additional addresses-linked addresses
- Directors data

POL00030670

- Commercial searches, (i.e. valuable data relating to the suspect's business.)

Land Registry. Investigators have access to the Land Registries in England and Wales, Scotland and Northern Ireland. Most searches take between a few minutes to a few days, depending on the registry. Obtaining the subject's full address is important. Land Registry can provide the following type of information/data:

- The owner(s), type of ownership & address
- The value of property
- An extract of the official Title Deed
- Copy of the Title Register, Title Plan
- Registered Old Deeds, including historical editions of the register and title plan
- Any charge on the property, and the relevant financial institution (mortgage.)

Network Business Support Centre (NBSC) Call Logs. NBSC call logs can be obtained by emailing the Branch and IT System Team at Dearne House. These logs will detail all calls made by a branch into the NBSC.These logs can be very useful where a SPMR or employee claim that they have reported the loss or incident.

Credence. Credence is a tool used to analyse detailed transactional data from a particular branch, this is useful to prove details of particular transactions or events. Only data, up to 90 days, can be extracted and analysed by Post Office Ltd Security. An Application to Fujitsu will turn the MI data into data/documentary evidence for use in the criminal courts. Older/historic data can be obtained too. Fujitsu will provide a witness statement relating to the authenticity of the data only, not the specific transactions relating to your enquiry.

ONCH. The Cash Management team can provide Over Night Cash Holdings (ONCH) data for a specific branch. This data gives in depth cash analysis for a branch including what denomination of notes a branch has declared on a given date along with cash remittances in and out. A request for this data can be made to the Retail Cash Management Team who will highlight any concerns they might have with the branch. The same information can be requested for Foreign Currency holdings.

Full Rota Check. A 'full rota check' allows for a full data search for a specific branch relating to transaction issues. This can include any transaction corrections (TC's) scratch card, remittances, stock adjustments and other specific office's products. This check can be arranged via Post

POL00030670

Office Ltd Security Grapevine strand, Analyst & Support team in Chesterfield.

Alarm Data
Obtaining alarm data from ROMEC can be a useful tool in determining access to the Post Office secure area and safes. Data around perimeter and safe set / unset times can be interrogated to assist in the investigation.

PLANNED OPERATION RISK ASSESSMENT (PORA)

The PORA process is mandatory in any Post Office led investigation which may involve a planned interview under caution or premises search. A PORA is required for each suspect involved in the investigation, In order to manage the risks effectively Investigators should conduct any risk related intelligence checks and/or enquiries that they feel are necessary as part of the PORA process. The following checks are available and thought to be the most relevant to Post Office Security cases:

- Local Management check: This may also identify other information such as health issues, including suspected drug or alcohol habits, or outside interests e.g. domestic circumstances which may impact on H&S.
- PNC Individual checks: This may identify "warning" indicators or previous convictions of both suspects and others at the address. It may also identify other information which impacts on H&S such as any history regarding the certification (or refusal) of firearms or orders recalling persons to hospital.
- Full Equifax check: This check can be used to identify current occupants at an address to be searched or visited. A "Full Investigation" Equifax check should be undertaken.
- PNC Vehicle check: This can reveal registered keepers of vehicles at a specific address.
- Land Registry checks: These will identify the owner of property.
- Local Police Intelligence check: May identify risks regarding the suspect or other incidents or persons at the address(es) and the geographical area(s) to be visited. It may also identify other law enforcement interest.

Risk Score. Where any risk is assessed as High, a Senior Security Manager should be consulted and the assistance of the Police sought before any investigation activities which bring Investigators into contact with the suspect are commenced.

Where the Planned Operation is assessed as Low or Medium risk, line manager's authority must be obtained before any investigation activities which bring Investigators into contact with the suspect are commenced.

POL00030670

INTERVIEW

Where the rights of a lawyer to be present are offered to the subject who wants their own solicitor and they are not available, consider your position in terms of recovering evidence and not compromising the investigation. In this instance inform the suspect that as their lawyer cannot attend within a reasonable time, arrange for the suspect to be arrested and booked in at the local police station where a solicitor from the nominated list or the duty solicitor can be offered.

Reasonable time may differ depending on the circumstances and any action taken needs to be justified and documented. It is likely that an explanation for this course of action will be required at court. A rule of thumb is what the average lay person may consider reasonable given all the facts. It is important to note that the need to gather evidence and investigate the case in a timely manner is not unduly compromised.

Arrest by the police may be justified on the basis that there are reasonable grounds to suspect an offence has been committed and there are reasonable grounds for believing that the arrest is necessary. The statutory criteria for what may constitute necessity are set out in para 2.9 of Code G PACE. Inviting the suspect to the police station to obtain legal representation may not be effective as the alleged offender is at liberty to leave at any time. The investigator should direct the investigation appropriately to remain in control of the evidential process without jeopardising the suspect's legal rights.

Consider maximising the opportunity to capture evidence at the earliest stage, ie where there is a significant comment. In more complex cases where a more in depth interview is required hold a preliminary interview, cover off the significant comment and hold a second interview at a later stage when more evidence is gathered. Think of the Golden Hour of capturing the evidence. Always follow the PEACE model [Planning, Engage and Explain, Account, clarification and challenge, Closure, Evaluation]. Consider the ingredients of the offence; dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it. Ensure that these are established during the interview. Deep dive into areas where defences are likely. These can be countered by careful planning and skilful questioning.

One on one interviewing should be considered on a case by case basis. There is no reason why in a straight forward investigation where there have been admissions and risk is

POL00030670

considered low, that a one on one tape recorded interview should not be considered. This will free up resources and should be encouraged wherever possible. Clearly in more complex cases, where there is a need to pre prepare and the nature of the investigation may benefit from an interviewer with greater subject knowledge, then the interview must be conducted by two persons. Similarly for training and development purposes.

Should the recent Second Sight review be brought up by a suspect or his representative during a PACE interview the Security Manager should state:
I will listen to any personal concerns or issues that you may have had with the Horizon system during the course of this interview

The following three areas need to be covered in as much detail as possible at an appropriate point during all PACE interviews, regardless of whether Horizon is mentioned or not. Where the case clearly has no link with Horizon (e.g. theft of mail) then you must gain authorisation from your line manager to proceed outside of this process.

- Training
- How long have they worked at the Post Office?
- Had they any previous PO experience?
- How long did their initial training last? (Please see guidance below and get as much detail as possible)
- What did it cover? (ie transactions, balancing, ATM, lottery etc)
- Did they request any follow up training? (if so who with?)
- Was there a period when the accounts balanced? If so, then why did things run smoothly then?
- Support
- Who did they tell that they were having problems?
- Why didn't they request any help?
- What support are they aware of (ie NBSC, HSH, area managers)
- Have they contacted the NBSC for support before?

- Horizon
- Have they contacted the HSH before?
- If they believed that there was a fault with Horizon then who did they report it to and when? If they didn't report it then why not?

NBSC call logs should be requested for all cases. As should HSH call logs.

Training records for all new cases are automatically sent by casework team. For info the current standard is:

POL00030670

- SPMR receives 6-8 days of classroom training (this depends on the products that their office transacts)
- SPMR receives 6 days of onsite training and support including at least one balance.
- SPMR receives an announced visit after one month to provide support, go through the compliance requirements and for a cash check to be completed.
- SPMR receives an announced visit after 3 months for further support, compliance questions and a cash check.
- SPMR receives an unannounced visit after 6 months for further support, compliance questions and a Financial Assurance audit.

SEARCHES

In all cases a search of vehicle and premises should be considered, searches are conducted by consent and should be conducted in the spirit of PACE where reasonable grounds to suspect there is evidence on the premises that relates to the offence.

If the subject refuses to consent to a voluntary search the investigators line manager should be contacted and if required further advice and guidance sought from the criminal law team.

If the subject refuses to consent to a voluntary search and there are reasonable grounds to suspect that evidence relating to the offence may be found, then contact police with a view to arrest the suspect. A search can then be conducted by police following arrest. The investigator should agree this course of action with their line manager and advice sought from the criminal law team.

NOTEBOOK

Notebooks are an essential element in a Security Managers toolkit. They are the recognised and preferred way of recording evidence that is not recorded elsewhere in a more formal document. They are numbered individually and are issued to all Investigators performing investigation duties.

Due to the nature of the information recorded in a notebook it can be produced, if required by the Investigator, in a Court of Law. It is essential that all notebooks be completed with a degree of uniform professionalism.

General rules

- Make all entries in chronological order.
- All entries must be made in ink (black preferably).

POL00030670

- Any errors must be crossed out with a single line, so that the original entry can be seen and then initialled.
- Do not remove any pages, they are all numbered sequentially.
- Do not make additional entries between the ruled lines. If it is of paramount importance that, if you make an additional entry, make it at the end of your existing entry explaining why it is not in chronological order.
- A single line should be scored through any blank spaces or lines.
- All entries should be signed, timed and dated.
- All notes made on informal pieces of paper such as newspapers, should be transferred to the notebook as soon as practicable. The entry should include why it was not practical to enter the note directly into the notebook. The Investigator must retain the original note.

POST INTERVIEW

48 Hour Offender Report: To be emailed to Team Leader, Casework Team, Financial Investigator (if appointed) Primary Stakeholder within 48 Hours of the interview.

FES Report: Financial Evaluation Sheet to be emailed to Financial Investigator within 48 hours of the interview.

Write the Case Summary Report: This is to be written using example report and guidelines that can be found on the Secps sharepoint site. The case summary should be a succinct chronological account of the investigation highlighting key facts. The rule of thumb is to produce an account which the reader can quickly digest to get a general overview of the allegation. Key witnesses and a brief outline of what they say can be included as well as a synopsis of what was said during interview. The statements, interview record and exhibit list can be examined should the reader require further information.

Write Discipline Report. Discipline report to be written using example report and guidelines.

INTERVIEW NOTES

In the majority of cases at initial submission, the Notes of interview need to be a brief account of the interview and any significant comment. It is therefore good practice to write down a note of the interview and generally what was said on completion.

An example note could be: throughout the interview the subject stated that he had borrowed the money to make up a shortfall and when challenged over this accepted that it was wrong/dishonest to take the money.

POL00030670

No comment interviews should not be transcribed. Unless there is a very good reason for a full transcript, in the majority of cases for the initial submission a note of interview will suffice.

Where the prosecuting lawyers request a transcript as part of the advice process or for preparation for committal proceedings it will be completed by the typist, checked and sent by the Security Manager.

Where appropriate to transcribe the Audio recording of an interview the request should be sent to the typist. An email should be sent to cathphilbin@aol.com. The email should also be copied to Helen Dickinson to ensure return of the CD.

STATEMENTS

In all instances the following standard statements should be taken and submitted with the green jacket.

- First Officer Statement
- Second officer Statement
- Horizon System Statement
- SPMR Contract Statement
- Lead Auditor Statement

In the course of an investigation other statements may need to be acquired, these could be statements to describe a particular process such as how to carry out a particular transaction. If the Post Office Legal and compliance Team (POLCT) consider that such a statement is required to progress the prosecution they will send an advice requesting this further information.

Where statements can be taken over the telephone this should be done to save time and resources and it must be encouraged. Statement taking over the telephone is an accepted and modern practice.

Rather than a hand written Section 9 statement, there is no reason why a draft statement cannot be prepared in note form. The statement can then be typed up subsequently, with any changes, clarification or ambiguity amended. It is vital that the original notes are retained. On typing up the statement it can be sent to the recipient for checking and amending. Once agreed, the statement must be signed and sent back to the investigator.

BUSINESS FAILINGS.

18.1. If business failings or procedural weaknesses are identified this should be completed on the relevant tab of

POL00030670

the new case raised form and emailed to all stakeholders including Commercial Security. This should be printed off and associated in appendix C of the file.

FILE CONSTRUCTION

A Green Jacket should be constructed as per the following guidelines.

Case files will include a schedule of unused non-sensitive material and unused sensitive material [Public Interest Immunity, Legal Privilege and documents that may highlight the methods used for investigation] The Appendix "C" in the case file will be retained by the Security Manager as oppose to submitted with the file. Where solicitors may wish to examine any unused material it should be requested and sent by the Security Manager.

The body of the file.

- Case Raised Front Sheet
- Event Log [added to as the case progress to conclusion]
- File Contents Index
- Case File summary; numbered paragraph.
- Index of Statements (Actual Statements in Appendix A)
- Interview Summary
- Index to Exhibits
- Unused Material list [This negates the need to submit Appendix C and fill the file with emails. The unused material list can be added to as the case progresses]

General Rule Appendix A = Witness Statement B = Evidence C = Other

Appendix A

- Typed Witness Statements
- Summons Documents

Appendix B

- POL001
- Evidence
- Notebook Entry
- Search Documents
- Working Tapes
- PNC check results (include no trace replies)

Appendix C (Appendix C should be collated, but NOT be submitted with the file when sent to the criminal law team)

- Stakeholder Notification

POL00030670

- HR Printout
- Assistant List
- Interview Letter
- POL003
- Business Failings
- Discipline Report
- Antecedents
- NPA01

FILE SUBMISSION

Cases for Advice.
In some instances where the investigator is unsure on the strength of the evidence the case can be submitted to the POLCT for advice. The POLCT will apply the evidential test and will advise on the next course of action such as further statements or case to be closed.

On completion of the file, it will be submitted to the team leader for checking, signing off and forwarded to the POLCT via registration. Should further investigation be deemed necessary at this stage, the file will be returned to the Security Manager. Where a request is made from POLCT for further enquiries, the team leader will be copied into the relevant email. It is imperative that the progress of enquiry document is comprehensively kept up to date and copies of any generated emails saved. These can be inserted into the file in appendix C when the enquiries are complete.

Should advice be sought from Cartwright King solicitors, the Team Leader and POLCT will be copied into any requests for further evidence. The details of investigation log must be maintained and copies of emails retained. On completion of the enquiry, the green docket case file will be sent to the Security Manager for copies of any emails to be inserted along with the progress of investigation log prior to final submission to Head of Security via the Team Leader.

Each case file should the follow the stated process:

- Security Manager > Team Leader > Post Office Legal and Compliance Team > Cartwright King > Head Of Security > Team Leader > Security Manager

Security Manager > Team Leader

- Once the file is ready for submission the investigator should send the green jacket to their Team Leader for review. The Team Leader should sense check the case file and ensure it is evidentially robust and properly constructed. The Security Manager should send electronic copies of the offender report, audio transcripts and discipline report to Post Office Security.

POL00030670

Team Leader > Post Office Legal and Compliance Team

- The Team Leader will then forward the file to the POLCT The file will be reviewed by the POLCT and a decision made whether further progression be made with the case. If the decision is No Further Action the file is returned to casework at that point (next step 5.6). If the POLCT decides that further enquiries are required this will be forwarded to the investigator including Casework and the Team Leader.

Post Office Legal and Compliance Team > Cartwright King

- If the decision is to proceed with the prosecution case the file is the forwarded to Cartwright King for advice on charges. (In some instances POLCT will put charges together).

Cartwright King > Post Office Legal and Compliance Team

- Cartwright King will prepare advice and charges for the case (or advise no further action). If further enquiries are required they will contact the investigator direct, copying in the team leader and send an advice detailing the further enquiries. The advice along with charges and case file is then sent back to casework.

Post Office Legal and Compliance Team > Head Of Security

- The file is then forwarded to the designated prosecution authority (DPA) for authority to proceed. The DPA will review the case file and decide whether to proceed with the advice from the POLCT and Cartwright King or whether to take a different course of action. The authority to proceed (or other instruction) will be inserted into the case file.

Head Of Security > Team Leader

- The file is the forwarded back to the casework team.

Team Leader > Security Manager.

- The file is returned to the investigating officer with advice and charges submitted in the case file for the Security Manager to proceed.

SUMMONS

If advice from Cartwright King or the POLCT is to prosecute and the Head of Security has given authority to proceed, then the investigator needs to obtain a summons.

POL00030670

The Security Manager will make contact with the relevant Magistrates' Court to set a date for the suspect's first appearance at court. Summonses are also applied for. Upon receipt of the summonses the Security Manager will serve the summonses by way of posting them to the suspect offender using the Royal Mail Special Delivery service.

Set a Court Date

- Contact the Magistrates court where the offence took place and confirm that court deals with the matter and the address where the summons are to be sent for signature..
- Contact listings and inform them you are a private prosecution - (certain courts have set days for non-police prosecutions).
- Obtain a date normally six weeks from date of request but no more than 8 weeks.

Acquiring Arrest Summons (AS) Number

- Update the front of the NPA01 with the date of the court hearing and the details of the court,
- Complete the offence and the method used in offence section on the front of the NPA01.
- Email the updated NPA01 (and NPA02 if required) to the casework team. The casework team will apply to the relevant police force for an AS Number which is required for the court to sign the summons. The AS number will be emailed back to the investigator within a few days of the submission of the NPA01 (different police forces work to different timescales to times will vary).

Applying for the summons.

- Prepare three copies of the summons
- Prepare one information sheet.
- Send to the court for signature with covering letter - all three copies of the summons should be signed and returned.
- Court will retain the information sheet.
- Inform the agents Solicitors appointed by POLCT of the time and date of the court appearance.

On receipt of the summons

- Take a photocopy of the defendant's copy of the summons.
- Send the original copy of the defendants summons together with a POL044 (Charge or summons notice) and a copy of the means form.
- Summons can be either served personally or via Royal Mail Special Delivery to the offender.

POL00030670

Once conformation has been obtained that the summons has been received POLCT and Cartwright King must be informed. The back of the defendants photocopied summons should be endorsed with the following:

- I certify that today, (date), I personally served a copy of the summons upon (Name), the defendant named overleaf.

or

- I certify that a copy of the summons overleaf has been served upon (Name), the defendant named overleaf. The summons was sent via Royal Mail Special Delivery (number) and was delivered (date and time).

Prepare and send to POLCT a covering letter confirming the summons has been served, together with a copy of the POL033 and any TIC's by post. Update the front of the NPA form with the summons was applied for and the date the summons was served. Complete the offence and the method used in offence on the front of the NPA01.

Email Casework team and POLCT the confirmation of service letter together with the NPA01. If the case is a FI case then the FI should be copied into the email.
.
Copies of the summons go in Appendix A of the file.

COMMITTAL

Committal Checklist
POL006B Self Disclosure
POL006c Schedule of non-sensitive unused material
Sensitive Material
Cont Disclosure Report
Witness List
Witness Address
Witness Non Availability
List Of Exhibits
Memo to POLCT

DEBARMANT

CASE CLOSURE

On completion of the investigation, it is vital that a review of the root cause of the investigation is undertaken by the Security Manager. It is important to ascertain whether any system processes, integrity of the financial commercial product, technical issues, training delivered or procedures may have provided an opportunity to commit the offence. Equally important, the vulnerability of the product or process in its current form and likelihood of similar offences being committed in the future needs to be

POL00030670

considered. A comprehensive report outlining the cause of the offence will be submitted to Commercial Security at the conclusion of each investigation.

As part of the Post Office retention policy, case files must be archived and retained for at least 7 years.

Case closed Notification.

- The Case Closed notification should be completed and emailed to the investigators team Leader, Post office Security all major stakeholders and Commercial Security team.
- As much detail as possible should be included in the case closed notification explaining the decision for the course of action taken.
- In some instances a case will be closed with no green jacket, this could be a case where the matter was dealt with under conduct and no criminality identified. If there is no green jacket this should be highlighted on the case close notification and also annotated at the top of the email to Post office Security.

One of the key programmes of the Security Operations strategic plan for 2013 has been the case file review. Separation from Royal Mail Group has presented opportunities to shed outmoded investigation practices and tailor processes that not only meet the current needs of the business, but challenges us as a team to work smarter, and deliver a professional, comprehensive and fair investigation in a timely manner. With the advent of the Second Sight interim report it is likely that scrutiny will continue to focus on the fairness, evidential quality and professional standard of criminal investigations. Completion of the investigation review, which serves as a guide to Security Managers in the conduct of their investigations is a timely document which embodies the ethos of Care, Challenge and Commit.

5 Exceptions

One of the key programmes of the Security Operations strategic plan for 2013 has been the case file review. Separation from Royal Mail Group has presented opportunities to shed outmoded investigation practices and tailor processes that not only meet the current needs of the business, but challenges us as a team to work smarter, and deliver a professional, comprehensive and fair investigation in a timely manner. With the advent of the Second Sight interim report it is likely that scrutiny will continue to

POL00030670

focus on the fairness, evidential quality and professional standard of criminal investigations. Completion of the investigation review, which serves as a guide to Security Managers in the conduct of their investigations is a timely document which embodies the ethos of Care, Challenge and Commit.

6 Violations

It is the responsibility of each system owner to make sure that they are keeping their departmental systems in compliance with the above stated policy. Failure to do so constitutes a violation of policy.

7 Enforcement

Post Office Security Operations Management will regularly assess for compliance against this policy. Any violation of this policy will be investigated and if the cause is found to be due to wilful disregard or negligence, it will be treated as a disciplinary offence. All disciplinary proceedings are coordinated through the Human Resources Department.

8 References

AEI	Application Enrolment Identity	NPA	Non Police Authority
AS	Arrest Summons	PACE	Police and Criminal Evidence Act 1984
ATM	Automated Teller Machine	PAH	Primary Account Holder
CCTV	Close Circuit Television	PEACE	
DPA	Designated Prosecution Authority	PNC	Police National Computer
DVLA	Department of Vehicle Licencing	POCA	Post Office Card Account
DWP	Department of Working Pensions	POL	Post Office LTD
ECF	Event Capture Form	POLCT	Post Office Legal and Compliance Team

POL00030670

FES	Financial Evaluation Summary	PORA	Planned Operation Risk Assessment
FI	Financial Investigator	ROMEC	
HP	Hewlett Packard	SPMR	Sub Postmaster
H&S	Health and Safety	TC	Transaction Correction
HSH	Horizon System Helpdesk		
NBSC	Network Business Support Centre		
NFSP	National Federation of Sub Postmasters		