Conduct of
Criminal Investigation
~~Policy~~Policy

Version No.	Reason for issue	Date
Version 1.0	First issue	04.04.2014
Version 2.0	reviewed & amended	28.08.2018
Version 2.1	Final draft	04.09.2018
Version 3.0	Adopted & issued	??.??.2018

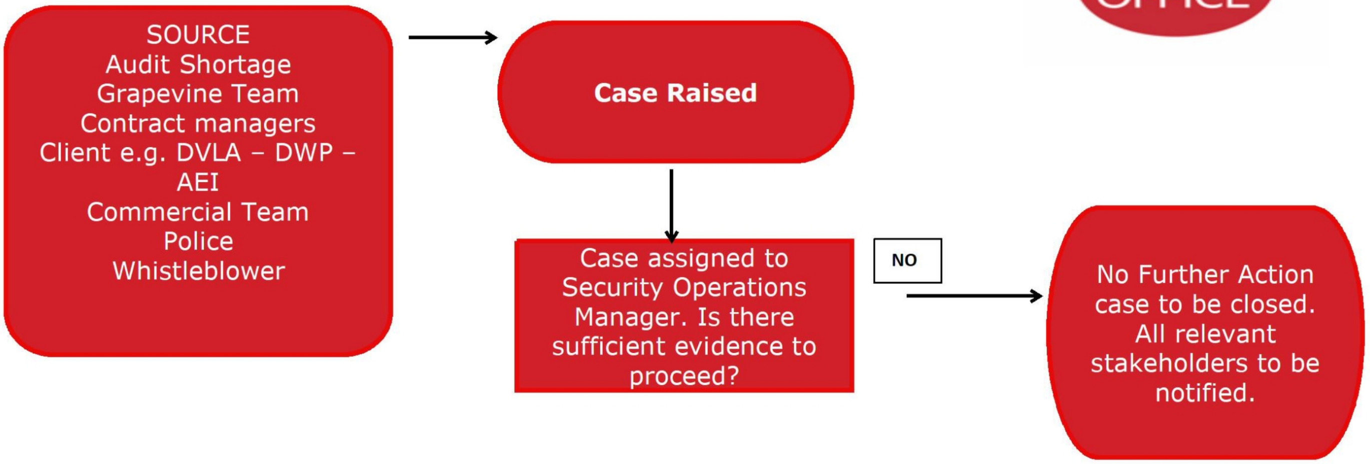
Table of Content

POL00126145

Glossary of Terms

AEI	Application Enrolment Identity
AS	Arrest Summons
ATM	Automated Teller Machine
CCTV	Close Circuit Television

DMB	Directly Managed Branch
DPA	Designated Prosecution Authority
DVLA	Department of Vehicle Licencing
DWP	Department of Working Pensions
ECF	Event Capture Form
FES	Financial Evaluation Summary
FI	Financial Investigator
HP	Hewlett Packard
H&S	Health and Safety
HSH	Horizon System Helpdesk
NBSC	Network Business Support Centre
NFSP	National Federation of Sub Postmasters
NPA	Non Police Authority
PACE	Police and Criminal Evidence Act 1984
PAH	Primary Account Holder
PEACE	Planning, Engage and Explain, Account, Challenge, Evaluation
PNC	Police National Computer
POCA	Post Office Card Account
POL	Post Office Ltd
POLCT	Post Office Legal and Compliance Team
PORA	Planned Operation Risk Assessment
SecOps	Security Operations
SPMR	Sub Postmaster
TC	Transaction Correction



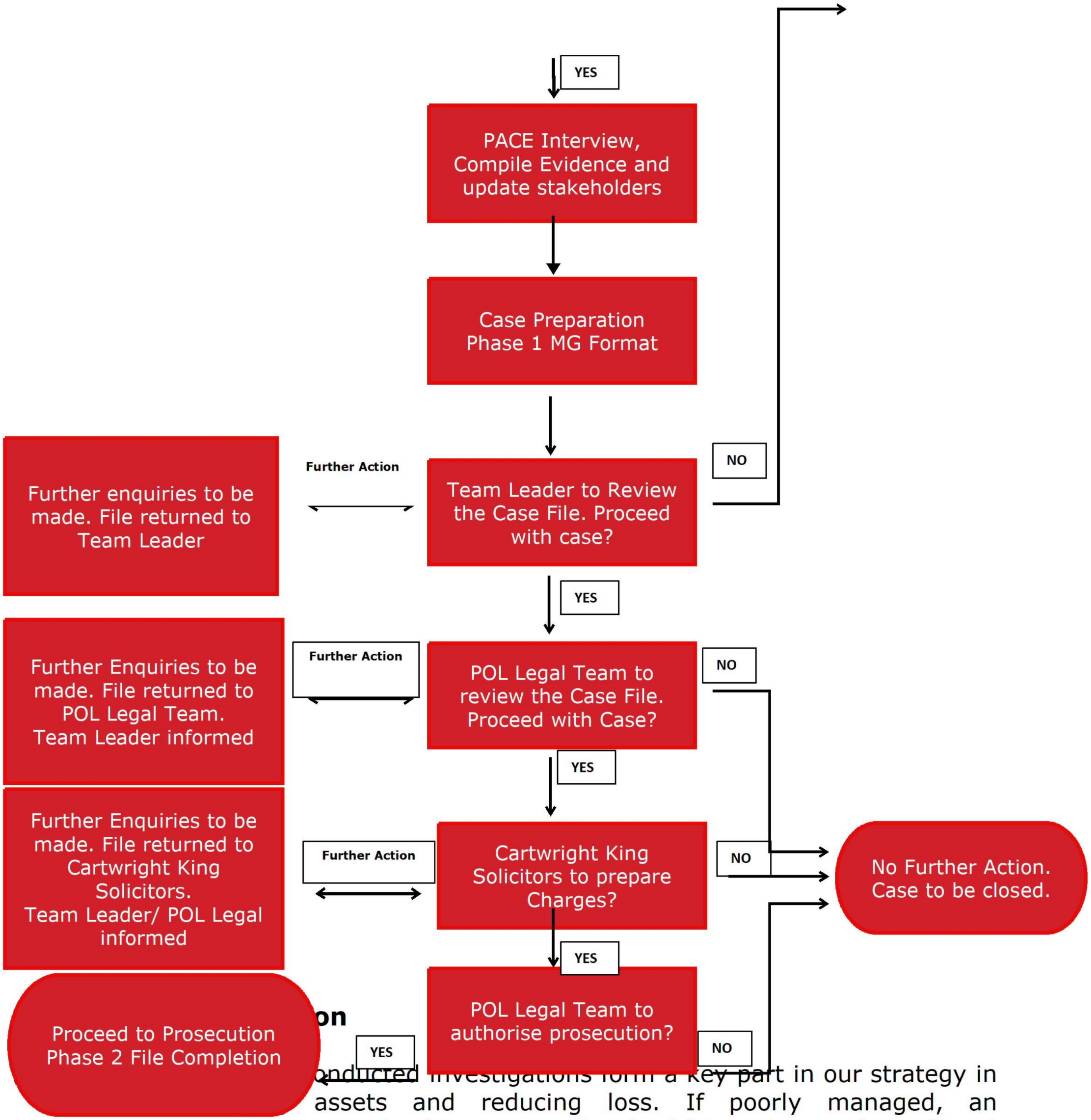
SOURCE
Audit Shortage
Grapevine Team
Contract managers
Client e.g. DVLA – DWP – AEI
Commercial Team
Police
Whistleblower

Case Raised

Case assigned to Security Operations Manager. Is there sufficient evidence to proceed?

NO

No Further Action case to be closed. All relevant stakeholders to be notified.


YES
PACE Interview, Compile Evidence and update stakeholders
Case Preparation Phase 1 MG Format
Further enquiries to be made. File returned to Team Leader
Further Action
Team Leader to Review the Case File. Proceed with case?
NO
YES
Further Enquiries to be made. File returned to POL Legal Team. Team Leader informed
Further Action
POL Legal Team to review the Case File. Proceed with Case?
NO
YES
Further Enquiries to be made. File returned to Cartwright King Solicitors. Team Leader/ POL Legal informed
Further Action
Cartwright King Solicitors to prepare Charges?
NO
No Further Action. Case to be closed.
YES
Proceed to Prosecution Phase 2 File Completion
YES
POL Legal Team to authorise prosecution?
NO

on

onducted investigations form a key part in our strategy in assets and reducing loss. If poorly managed, an investigation can lead to increased risk of future loss and significant damage to the corporate brand. When 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 Ltd Security Operations 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.

1.2. There is another anomaly that sets us aside from other commercial investigators. Of our 11,600 branches, only 350 are currently staffed by employees of Post Office Ltd. Branches are operated by either Franchisees, Agents or Limited Companies (Operators) who receive remuneration based upon transactions. As none are deemed to be employees of Post Office Ltd, the usual practices and procedures of an employer employee investigation do not apply.

4 1.3. In cases where ~~fraud~~ suspected misconduct [SC1]is uncovered and good evidence of criminality exists, a criminal investigation will invariably commence. At the same time Post Office Ltd 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 Operations 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.

1.4. 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. The Purpose

2.1. This guide been prepared as part of the case file review and is intended to support Security Operations Managers from the commencement through to the conclusion of an investigation. Included in the document is comprehensive guidance of the process including key points to consider at various stages of the investigation.

2.2. Prior to commencing an investigation the Security Operations Manager will have to consider:

5 - The seriousness of the allegation, to be determined by a consideration of those factors set out at paragraph 6.3 of Post Office Limited's Prosecution Policy[SC2].
6 - The level of criminality to be determined by a consideration of factors i. to iv., vi. to viii., x. and xiv. set out at paragraph 6.3 of Post Office Limited's Prosecution Policy.[SC3].
- Any contractual, compliance or regulatory concerns.
- The potential to damage the reputation of Post Office Ltd.
- The expectations of key stakeholders.

Page 5 Comments

SC1 See paragraph 12.1 of Review document.
Simon Clarke, 25/08/2018 04:36 PM

SC2 See para.2.2 of Review document.
Simon Clarke, 25/08/2018 04:41 PM

SC3 See para.2.2 of Review document.
Simon Clarke, 25/08/2018 04:41 PM

3. Case Raised

3.1. Cases are raised from various sources. In each instance the information is passed to the relevant operational Team Leader who will evaluate the circumstances and decide whether or not a ~~fraud~~ criminal investigation case should be raised.

3.2. 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 through to Post Office Security Operations 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.

3.3. 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 individual circumstances and assess whether an investigation is the most suitable course of action working in conjunction with the Contract Manager.

3.4. The following are examples of types of audit shortages although the list is not exhaustive.

- Cash Shortage at Audit - no explanation.
- Cash Shortage at Audit - comments made during the audit.
- Cash Shortage – member of staff (not the Operator) suspected of criminality.
- Cash Shortage – Loss hidden transfers.
- Cash Shortage – Loss hidden remittances.
- Cash Shortage – Loss hidden cheque suppression.
- Personal cheque in drawer.
- Cash Shortage in ATM.
- Cash Shortage in Lottery.

3.5. Post Office Card Account (POCA) cases; On occasion, the service provider 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 service provider who, working on behalf of Post Office Ltd, manage the day-to-day POCA service. The service provider is 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 will 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 Security Admin 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 a member of their team for further investigation.

3.6. Cases can be raised in relation to a specific client; these can come from various sources including directly from the client, via the Financial Crime Team, a complaint from a customer or analysis from the Fraud Analyst or Grapevine Team. In each case the request is emailed to the Team Leader to review the circumstances and assess whether an investigation should take place. Post Office Ltd has a varied client base; the following are examples of sources from where cases are usually raised:

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

3.7. Cases also can be raised from various other sources including:

- DMB Issues / Loss
- Suspicious Transactions
- Remuneration (Banking or Mail products)
- Contracts Manager
- Police Requests
- Whistleblower

3.8. 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 Security Admin Support Team via email that a case is to be raised and which Security Operations Manager has been nominated to deal with the case.

3.9. The Security Admin Support Team then complete the new case raised document and email this to the relevant Security Operations Manager along with any ECF or audit reports which they have received.

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

3.11. Once a case has been raised an email should be sent to all stakeholders by the Security Admin Support Team ensuring that as much detailed information is included as possible. Further updates will be circulated by the Security Operations Manager via the Security Admin Support Team.

3.12. Communication with the Financial Crime Team is essential. It is important to ensure that all stakeholder updates throughout the investigation are copied to the Financial Crime team including details of any product or procedural weaknesses.

4. Event Log

4.1. All activities undertaken during an investigation should be continually recorded on the event log on Sharepoint within the electronic case file; this should also[SC4] include reasons for any delay in the progression of a case. Entries in the Event Log must be timed and dated and must be signed or initialled by the person who conducted the relevant activity. 8, 9

5. Supervision of Investigation

5.1. 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, additional auditing, a caution, warning letter and / or NFSP engagement. Some of these possible outcomes may not be obviously apparent until the subject has been interviewed under caution. The investigation should be continually assessed and outcomes should be considered at this early opportunity. Close communication and co-operation with key stakeholders is essential to ensure that a proper and considered course of action is taken.

5.2. Consistent supervision and review is vital to ensure that cases are thoroughly investigated and submitted in a timely manner. Team Leaders need to quality assure investigations making sure prior to initial submission that all available evidence has been produced.

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

6. Investigation

6.1. It is important to consider the aims, objectives and scope of the investigation. Not all Post Office investigations are criminal; the

Page 8 Comments

SC4 Reinforces the need to make contemporaneous or near-contemporaneous records of activity. Is also good practice.
Simon Clarke, 25/08/2018 04:49 PM

Security Operations 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 route of an investigation. An example may be a Flag Case where senior stakeholders would have an on-going interest in the progression of the investigation.

6.2. When a case is raised, the Security Operations Manager needs [SC5] to prepare an investigation plan which will outline the way the investigation will be conducted. Points to consider include:

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

6.3. In all cases stakeholder engagement is essential. Updates to stakeholders should be given on a regular basis, particularly following an interview, file submission and summons served. For cases against employees such as DMB losses, updates should be more frequent and include key senior stakeholders in the relevant directorate.

6.4. For cases raised due to an 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 cause of the loss. Also the auditor should be instructed to produce all relevant audit documentation (original documentation) to the Security Operations Manager.

6.5. In all cases where a loss has been identified and an operator has been suspended, a case conference should be arranged with the Contracts Manager at the earliest opportunity. This is essential to allow for an exchange of information and understanding of expectations and direction the Contract Manager is planning in relation to disciplinary action. The contract process can be found in Appendix A.

6.6. There may be occasions where criminality is suspected that a request is made directly to a Contract Manager to consider suspending the operator. In these circumstances the Security Operations Manager must provide a detailed explanation outlining the rationale to support the request. A record must be kept of this

Page 9 Comments

SC5 Grammatical correction
Simon Clarke, 25/08/2018 04:49 PM

decision which may, at a future stage have to be produced in court proceedings.

6.7. The Security Operations Manager is tasked to identify whether a
11 ~~fraud~~ criminal offence has taken place. 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 or dispel the claim. 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 issues. A key point to cover template has been produced to ensure that Security Operations Managers establish these facts during the interview process. As part of the evidence gathering process, the Security Operations Manager should collect evidence from various sources including:

- Statements from witnesses [current, previous members of staff]
- Expert witnesses
- Post Office accounting and HR databases
- Dynamics 365 / Cloud City database
- CCTV
- Banking records
- Telephone records
- Interviews with suspects
- Alarm Data

6.8. 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 investigation event log.

12 6.9. The Security Operations Manager should open two schedules: SC6

13 - a Schedule of Non-sensitive Unused Material, upon which is to be recorded all investigation material obtained during the course of the investigation, but which is not evidence relied upon in the prosecution or is sensitive material as described in the sub-paragraph immediately below; and

14 - a Schedule of Sensitive Unused Material, upon which is recorded material which is not to be disclosed to the defendant without an order of the Court. Such material would, if disclosed, reveal sensitive investigative techniques and tools the publication of which would be likely to undermine future investigations. Classes of material to be recorded in this schedule includes, but is not limited to, requests for PNC Reports, information relating to investigative methods employed in the investigation, financial enquiry tools used,

Page 10 Comments

SC6 See paragraph 12.1 (6.9) of the Review document.
Simon Clarke, 25/08/2018 05:03 PM

legally privileged material, case analysis used for risk assessment or other legitimate internal purposes only. Neither the material in this schedule nor the schedule itself would be seen by a defendant unless a Court ordered it.

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

7. Enquiry Type

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

7.2. Major Enquiry >£75,000 (or major customer / client / reputation impact) where immediate response is not possible due to the requirement to perform pre-interview enquiries / analysis.

7.3. 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.

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

8. Interview Framework and Timescales

15 8.1. All ~~significant~~ SC7 steps in the investigation including any lengthy
delays in concluding enquiries need to be recorded in the event log.
16 The event log should be ~~disclosed as unused material~~ recorded in the
Schedule of Non-sensitive Unused Material SC8. The details of the
investigation need to be sufficiently informative although an element
of objectivity needs to be applied.

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

8.3. A culture is embedded where Security Operations 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

Page 11 Comments

SC7 To leave a step out, however seemingly insignificant at the time, invites criticism. It may be that an apparently insignificant step later assumes far greater importance. Leaving steps out also tends to undermine the integrity of the Event Log.

Simon Clarke, 25/08/2018 05:04 PM

SC8 Not all material is automatically disclosable – but all material should be recorded in one of the Unused Schedules. Only material which meets the test for disclosure (see page 4, footnote 8 of Review document) must be disclosed.

Simon Clarke, 25/08/2018 05:06 PM

the case at some later stage which may undermine the likelihood of successful prosecution.

8.4. Interview Date. The suspect should be contacted and invited to interview without undue 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.

8.5. Immediate Open Enquiry. Interview on day of notification or as soon as possible and case submitted to normal report timescales (12 days after interview).

8.6. Major Enquiry. Suspect to be interviewed within 1 month of case being raised and case submitted to normal report timescales (12 days after interview).

8.7. Standard Enquiry. Suspect to be interviewed within 2 months of case being raise and case submitted to normal report timescales (12 days after interview). Should enquiries indicate increased loss or impact, status must be amended to Major Enquiry immediately.

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

8.9. Security Operations Managers should discuss the case with their Team Leader on a minimum of a monthly basis and a way forward agreed and communicated. This will ensure that all cases are progressed and all stakeholders are continually updated.

9. Evidence

9.1. Good communication with the audit team is crucial to ensure evidential resilience in relation to the continuity of evidence. Every effort must be made to ensure that the person identifying is the person exhibiting any original documents. These will form the evidential basis of the case and should be securely stored at all times. To evidence continuity all evidence identified should be
18 produced and retained in a signed, sealed SC9 and dated exhibit bag. In circumstances where the only viable way is to send evidence through the post, this should be sent to the Security Operations Manager by Special Delivery.

19 9.2. Auditors ~~are encouraged to~~ should always SC10 record any significant comment made during the course of the audit either unsolicited or in

Page 12 Comments

SC9 Best practice.
Simon Clarke, 25/08/2018 05:11 PM

SC10 The absence of a contemporaneous or near-contemporaneous record will almost always result in exclusion by the court.
Simon Clarke, 25/08/2018 05:11 PM

response to a reasonable question. Examples are "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 i.e. "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.

9.3. In such cases, the Auditor should inform the subject that their comment will be recorded but any further questions concerning the comment should be discussed with a Security Operations Manager who will explain their legal rights. This should not detract from the role of the Auditor and questions should still be asked to allow them
20 to verify financial assets due to Post Office Ltd. In this respect Auditors are entitled to, and should, ask questions which: seek to identify persons present, go solely to the location of Post Office Limited's property or assets ("Is there any more cash on the premises?", "Where is X?"); questions about who owns a particular item; and questions for which the answers are necessary to complete the audit process. All other questions should be avoided.

9.4. In cases where the subject wishes to make comment, the Auditor
21 again should first explain that the subject has the right not to do so. If the subject is determined to comment, then the Auditor should
22 record the initial comment. They should then further advise the subject as above and if they still continue to comment, note in the record that the person concerned was advised that they would have the opportunity to discuss the matter with a Security Operations Manager. Any questions from the Auditor other than what are required to complete the audit would render the evidence inadmissible. The Auditor must refrain from engaging in a discussion relating to a shortage.

10. Background Checks

10.1. **Local Management Checks**; Contact with the Contract Manager is essential as they may have first-hand knowledge of the branch and operator. The Cloud City database can provide the Security Operations Manager with background information relating to the branch.

10.2. **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 by the operator when he was appointed to the branch. It will also show any intervention training requested or delivered for the branch. It is the operator's responsibility to register and train their own staff. No records of

Page 13 Comments

SC11 Added for the sake of clarity: not all questions amount to an ‘interview’ for the purposes of PACE.
Simon Clarke, 25/08/2018 05:21 PM

training (apart from compliance training) are kept for operators assistants.

10.3. **Post Office Ltd HR Personnel Print**. The personnel print should be obtained for all cases by emailing 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 operator was appointed
- Claims data i.e. holiday dates the operator was on holiday.
- The operator's full file can be requested by emailing 'Contract Admin Team'.

10.4. **P356 Data**. The P356 Data should be requested at the same time as the personnel print from the HR Assistants Check email address. This report can provide the following information

- All registered users at that branch.
- Name, date of birth and NI numbers.
- The Horizon user id's for each assistant
- Whether the assistant is permanently employed or temporary/holiday relief.
- Start and end dates of employment.

10.5. **Operators Remuneration.** The remuneration from any particular branch can be obtained via an e-mail to HR Agent Remuneration.

10.6. **Police National Computer (PNC).** Post Office Ltd 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 or known to be involved in committing criminal offences against Post Office Ltd.
- For operational Health & Safety considerations and evaluations prior to the engagement with the person concerned 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 Post Office Ltd.
  To identify the registered keeper of vehicles connected to the address of a suspected or known offender involved in criminal offences against the Post Office Ltd.

PNC checks must not be submitted 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.

10.7. **Equifax**: Security Operations Managers can rely on Equifax to provide the following information:

- Personal details.
- Addresses.
- Court and Insolvency Information, (i.e. County Court Judgments CCJ's).
- 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.
- Company Directors data.
- Commercial searches, (i.e. data relating to the subject's business).

10.8. **Land Registry**. Security Operations Managers have access to the Land Registries in England and Wales, Scotland and Northern Ireland. Most searches take only a few minutes but Scotland and NI have a different process and these can take much longer. Land Registry can provide the following type of information/data:

- The owner(s), type of ownership & address.
- The purchase price 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.)

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

10.10. **Credence**; is a system 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 also be obtained. Fujitsu will only provide a witness statement relating to the authenticity of the data only, not the specific transactions relating to your enquiry.

10.11. **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 can also highlight any concerns they might have with the branch. The same information can be requested for Foreign Currency holdings.

10.12. **Branch Check:** This can be requested from the Fraud Analyst Team and involves a full data search for a specific branch relating to transactional issues. This can include any transaction corrections (TC's) remittances, stock adjustments or any other specific office's products.

10.13. **Alarm data**. Obtaining alarm data from Grapevine 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.

11. Planned Operation Risk Assessment (PORA)

11.1. 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 subject involved in the investigation. In order to manage the risks effectively Security Operations Managers 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 interest's 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.
- PNC Vehicle check: This can reveal registered keepers of vehicles at a specific address.
- Land Registry checks: These will identify the owner(s) of a property.
- Local Police Intelligence check: May identify risks regarding the suspect or other incidents or persons at the address(s) and the geographical area(s) to be visited. It may also identify other law enforcement interest.

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

11.3. Where the Planned Operation is assessed as Low or Medium risk, line manager's authority must be obtained before any activities which bring Security Operations Managers into contact with the subject are commenced.

12. PACE Interview

23 12.1 Interviews should always be conducted within the provisions of
Code C paragraphs C.11 and C.12 of the PACE Codes of Practice.
Paragraphs C.11 and C.12 are appended to and form part of this
SC12
Policy. The right to legal advice must be offered to the subject from
the outset. If they want their own Solicitor and they are not
24 available, the Security Operations Manager should consider their
position in terms of recovering evidence and not compromising the investigation. In this instance advice should be sought from the Team Leader or Head of Security Operations on how to progress. Reasonable time may differ depending on the circumstances and any action taken would need to be justified and documented on the event log. 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.

12.1.

12.2. 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
SC13
25 are set out in para 2.~~9~~ 4 of Code G PACE. Inviting the subject to the

Page 17 Comments

SC12 Reflects the law and avoids inadvertent breach.
Simon Clarke, 25/08/2018 05:28 PM

SC13 Corrected.
Simon Clarke, 25/08/2018 05:29 PM

police station to obtain legal representation may not be effective as the person concerned is at liberty to leave at any time. The Security Operations Manager should direct the investigation appropriately to remain in control of the evidential process without jeopardising the subject's legal rights. Code G of PACE is laid out at Appendix B.

12.3. Consider maximising the opportunity to capture evidence at the earliest stage, i.e. where there is a significant comment. In more complex cases where a more ~~in depth~~in-depth interview is required, hold a preliminary interview to cover off any significant comment. Then hold a second interview at a later stage when more evidence has been gathered. 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. A comprehensive guide to interviewing using the PEACE model can be found at Appendix C.

12.4. Should the Horizon system be challenged by a subject or his representative during a PACE interview, the Security Operations 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'.

12.5. The following three areas need to be covered in as much detail as possible at an appropriate point during all PACE interviews.

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? (I.e. 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

- Did they tell anyone that they were having problems, if so who?
- If not, why didn't they request any help?
- What support are they aware of (i.e. NBSC, NFSP, HSH, area managers)
- Have they contacted the NBSC for advice or support before?

Horizon

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

12.6. NBSC and HSH call logs should be requested for all cases.

12.7. Training records for all new cases are automatically sent by Security Admin Team. For info the current standard is:

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

13. Searches

13.1. In all cases a search of vehicle and premises should be considered. All searches are voluntary 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. Consent should be documented prior to the search commencing.

13.2. If the subject refuses to consent to a voluntary search the Team Leader should be contacted and if required further advice and guidance sought from POL legal team.

13.3. 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 at risk, then advice should be sought from the police. The Security Operations Manager should agree any course of action with their Team Leader and advice may be sought from POL Legal team.

14. Notebook

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

14.2. Due to the nature of the information recorded in a notebook, it can be referred to by the Security Operations Manager, in a Court of Law. It is essential that all notebooks be completed with a degree of uniform professionalism.

14.3. **General rules**

- Make all entries in chronological order.
- All entries must be made in ink (black preferably).
- 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 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 by all concerned.
- All rough notes 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 Security Operations Manager must retain the original note.

15. Post Interview

15.1. 48 Hour Offender Report: To be completed on the electronic casefile on sharepoint and emailed to Team Leader, Security Admin Team and Primary Stakeholders within 48 Hours of the interview.

15.2. FES Report: Financial Evaluation Sheet to be completed on the electronic casefile on sharepoint within 48 hours of the interview.

15.3. Case Summary Report: This is to be written using example report and guidelines that can be found on the Security Operations 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 said 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.

15.4. Discipline Report. The discipline report should contain no legal jargon or opinion. It should be uploaded into the electronic casefile at

Appendix C and shared with the Contract Manager via Security Admin.

16. Interview Notes

16.1. In the majority of cases the MG report should be a complete Notes of interview need to be a brief account of the interview and any significant comment.

16.2. 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 the team leader and ensure return of the CD. All returns must be proof read by the Security Operations Manager and amended where necessary.

17. Statements

17.1. In all instances the following standard statements should be taken and uploaded into the electronic casefile at Appendix A.

- First Officer Statement
- Second Officer Statement
- Horizon System Statement
- Operator Contract Statement
- Lead Auditor Statement

17.2. 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.

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

17.4. Rather than a handwritten 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 26 are retained and a relevant entry made in the Schedule of Non-sensitive Unused Material[SC14]. Once typed, the statement can be sent to the recipient for checking and amending where necessary. Once agreed, the statement must be signed and sent back to the Security Operations Manager.

18. Business Failings

Page 21 Comments

SC14 See notes to paragraph 6.9 above.
Simon Clarke, 25/08/2018 05:30 PM

18.1. All business failings or procedural weaknesses should be raised by completing the relevant tab of the case raised form on sharepoint before emailing it to all stakeholders including the Financial Crime Team.

19. Electronic Case File Presentation

19.1. 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]. These should be scanned and uploaded to Appendix 'C' in the electronic case file with all originals being securely stored by the Security Operations Manager. Should Solicitors may wish to examine any unused material, it should be presented by the Security Operations Manager.

19.2. As a general rule Appendix; A = Witness Statement B = Evidence C = Other material

19.3. Appendix A

- Typed Witness Statements
- Summons Documents

19.4. Appendix B

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

19.5. Appendix C

- Stakeholder Notification
- HR Printout
- Assistant List
- Interview Letter
- POL003
- Business Failings
- Discipline Report
- Antecedents
- NPA01
- Unused material

20. File Submission

20.1. All cases should be submitted electronically to the Team Leader for review and advice. Once the evidential test is met, the case will be submitted to the Head of Security Operations and then POL Legal Team for advice on charges.

20.2. Should further investigation be deemed necessary at this stage, the Team Leader will be copied into the requesting email. It is imperative that the case event log is comprehensively maintained and copies of any generated emails saved. These must be uploaded to sharepoint along with all other relevant documentation.

20.3. If advice is sought from Cartwright King Solicitors, the Team Leader and POL Legal team will be copied into any requests for further information or evidence.

20.4. Each case file should follow the stated process:

Security Operations Manager > Team Leader > Head of Security Operations > Post Office Ltd Legal Team > Cartwright King Solicitors > Team Leader > Security Operations Manager

20.5. Security Operations Manager > Team Leader

Once the case is ready for submission, the Security Operations Manager should submit this electronically to their Team Leader for review. The Team Leader should sense check the case file and ensure that it is evidentially robust.

20.6. Team Leader > Head of Security Operations

The case will be discussed and reviewed by the Team Leader and the Head of Security Operations. All options will be considered but if charges are considered appropriate, the case will be submitted to POL Legal Team. The case will be reviewed by POL Legal Team and a decision made whether to progress the case to prosecution. If the decision is 'No Further Action' the Security Operations Manager and Team Leader will be informed. If POL Legal Team decides that further enquiries are required, the Security Operations Manager will be informed along with Security Admin and the Team Leader.

20.7. Post Office Legal Team > Cartwright King Solicitors

If the decision is to proceed with a prosecution, suggested charges will be agreed before the case is forwarded to Cartwright King Solicitors for advice on charges.

20.8. Cartwright King Solicitors > Post Office Ltd Legal Team

Cartwright King Solicitors will prepare advice on charges (or advise no further action). If further enquiries are required they will contact the Security Operations Manager directly to discuss. An advice note will be prepared copying in the Team Leader detailing the further enquiries. The advice along with agreed charges will then be communicated to Security Admin, POL Legal Team, Security Operations Manager and Team Leader.

20.9. Post Office Ltd Legal Team > Head of Security Operations

The case 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 POL Legal Team and Cartwright King Solicitors or whether to take a different course of action.

20.10. Head of Security > Team Leader

The file is referred back to the Security Admin team.

20.11. Team Leader > Security Operations Manager.

The case is returned with advice on charges to the Security Operations Manager to proceed.

21. Summons

21.1. If advice from Cartwright King Solicitors or POL Legal Team is to prosecute and the Head of Security Operations has given authority to proceed, then the Security Operations Manager will need to raise a summons.

21.2. The Security Operations Manager must contact the relevant Magistrates' Court to set a date for the suspect's first appearance. This should normally be six weeks from date of request but no more than 8 weeks.

21.3. Confirm the date with Cartwright King Solicitors to ensure that they can attend. Summons and laying of information to be prepared and once validated by the court, the Security Operations Manager will serve the summonses. This can be in person or by posting them using the Royal Mail Special Delivery service. Send the original copy of the defendants summons together with a POL044 (Charge or summons notice) and a copy of the Means form.

21.4. 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 to the Security Admin team who 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 Security Operations Manager within a few days of the submission of the NPA01 (different police forces work to different timescales to times will vary).

21.5. Once conformation has been obtained that the summons has been received, POL Legal Team and Cartwright King Solicitors 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).*

21.6. Prepare and send to POL Legal Team a covering letter confirming the summons has been served, together with a copy of the POL033 and any TICs. Update the front of the NPA01 form with the date the summons was applied for and the date the summons was served.

21.7. Security Operations Manager to email the Security Admin and POL Legal Team confirmation of service letter together with the NPA01.

21.8. Copies of the summons should be uploaded to Appendix A.

22. Committal

- Committal Checklist
- POL006B Self Disclosure
- POL006c Schedule of non-sensitive unused material
- Sensitive Material
- Continued Disclosure Report
- Witness List
- Confidential witness list
- Witness Non Availability
- List of Exhibits
- Memo to POL Legal Team

23. CASE CLOSURE

23.1. On completion of the investigation, it is vital that a review of the root cause of the ~~fraud~~ offence is undertaken by the Security Operations Manager. It is important to ascertain whether any system processes, integrity of the financial commercial product, technical issues, training delivered or procedures have contributed to 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 considered. A comprehensive report outlining the cause of the offence will be submitted to Financial Crime at the conclusion of each investigation.

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

23.3. Case Closed Notification.

- In all cases where a decision is taken to close a case it must be authorised by the Team Leader.
- The Case Closed notification should be completed and emailed to the Team Leader, Security Admin, all major stakeholders and the Financial Crime Team.

23.4 As much detail as possible should be included in the case closure notification explaining the decision for the course of action taken.

23.5 In the event of no further action, a standard letter should be sent to the subject informing them of the decision. A copy of this should be uploaded to Appendix C on sharepoint.

24. Conclusion

24.1. Completion of the investigation review, which serves as a guide to Security Operations Managers in the conduct of their investigations is a timely document which embodies the ethos of Care, Challenge and Commit. All guidance and considerations should be within the spirit of PACE 1984 Codes of Practice.

Track Changes

1	Change	*Simon Clarke,*	*04/09/2018 09:42 AM*
2	Insert	*Simon Clarke,*	*04/09/2018 09:43 AM*
3	Insert	*Simon Clarke,*	*04/09/2018 09:46 AM*
4	Change	*Simon Clarke,*	*25/08/2018 04:36 PM*
5	Insert	*Simon Clarke,*	*25/08/2018 04:40 PM*
6	Insert	*Simon Clarke,*	*25/08/2018 04:44 PM*
7	Change	*Simon Clarke,*	*25/08/2018 04:37 PM*
8	Insert	*Simon Clarke,*	*25/08/2018 04:47 PM*
9	Insert	*Simon Clarke,*	*25/08/2018 04:48 PM*
10	Insert	*Simon Clarke,*	*25/08/2018 04:49 PM*
11	Change	*Simon Clarke,*	*25/08/2018 04:38 PM*
12	Insert	*Simon Clarke,*	*25/08/2018 04:53 PM*
13	Insert	*Simon Clarke,*	*25/08/2018 04:53 PM*
14	Insert	*Simon Clarke,*	*25/08/2018 05:10 PM*
15	Delete	*Simon Clarke,*	*25/08/2018 05:04 PM*
16	Change	*Simon Clarke,*	*25/08/2018 05:06 PM*
17	Change	*Simon Clarke,*	*25/08/2018 05:08 PM*
18	Insert	*Simon Clarke,*	*25/08/2018 05:10 PM*
19	Change	*Simon Clarke,*	*25/08/2018 05:11 PM*
20	Insert	*Simon Clarke,*	*25/08/2018 05:21 PM*
21	Insert	*Simon Clarke,*	*25/08/2018 05:22 PM*
22	Insert	*Simon Clarke,*	*25/08/2018 05:22 PM*
23	Insert	*Simon Clarke,*	*25/08/2018 05:28 PM*
24	Insert	*Simon Clarke,*	*25/08/2018 05:26 PM*
25	Change	*Simon Clarke,*	*25/08/2018 05:29 PM*
26	Insert	*Simon Clarke,*	*25/08/2018 05:30 PM*
27	Change	*Simon Clarke,*	*25/08/2018 04:39 PM*