POLICE SCOTLAND
Keeping people safe

Fraud and Economic Crime

Standard Operating Procedures

Notice:

This document has been made available through the Police Service of Scotland Freedom of Information Publication Scheme. It should not be utilised as guidance or instruction by any police officer or employee as it may have been redacted due to legal exemptions

Owning Department	Specialist Crime Division
Version Number	4.00 (Publication Scheme)
Date Published	25/01/2018

Compliance Record

Equality Impact Assessment: Date Completed / Reviewed:	15/08/2017
Information Management Compliant:	Yes
Health and Safety Compliant:	Yes
Publication Scheme Compliant:	Yes

Version Control Table

Version Number	History of Amendments	Date
V1.00	Initial authorised version	15/03/2013
V2.00	Amended to reflect changes to current working practices. Insertion of Boiler Room Fraud information and information regarding Skimming Devices. Insertion of contact details for Scottish Crime Campus Gartcosh.	07/10/2015
V3.00	Change of contact details for ECU, Edinburgh (E and J division)	20/01/2016
V4.00	Amendment to include references to Public Sector Corruption, Bribery and Defalcation. Changes to Appendices to introduce greater clarity through use of flow-charts	12/12/2017

Contents

Appendices

1. Purpose

1.1 This Standard Operating Procedure (SOP) supports the Police Service of Scotland, hereafter referred to as Police Scotland, Policies for :

- Crime Investigation
- Serious and Organised Crime

1.2 It outlines the basic processes to be followed by Police Scotland staff upon receipt of an allegation of Fraud and when conducting enquiries into instances of Fraud and Economic Crime.

1.3 While some traditional Modus Operandi (MO) remain, others are constantly developing. Officers should keep an open mind when dealing with Fraud. This document is not intended to be guidance for every eventuality but identifies common themes and appropriate lines of enquiry.

2. Introduction

2.1 Common Law Fraud has three elements:

- Falsehood;
- Fraud;

  and
- Wilful imposition.

2.2 Forgery, Fraud, False pretence and Uttering (tendering as genuine) are treated in the main as different elements of the same crime i.e Fraud. Although it can take various forms, Fraud always has three elements:

- Pretence – the falsehood or deceit;
- Inducement – the persuasion or bait;
- Result – a definite practical effect.

2.3 The inducement is the link between the pretence and the result in order to establish the crime; it must be proved that the pretence did, in fact induce the result. However, in cases of attempted fraud it must be shown that the pretence, had it been effective, would have induced the result.

2.4 Most frauds result in the appropriation of goods or money but such appropriation is not an essential ingredient of the crime. In simplistic terms, it is sufficient that the victim has been induced by the pretence to do something that he/she would not otherwise have done.

2.5 Certain Fraud related offences are covered by statute. Statutory offences include possession or provision of articles for use in Fraud, false monetary instruments and false identity documents

2.6 In certain circumstances an assessment may establish that no actual crime has been committed. It may be prudent to inform the reporter that although the conduct described amounts to a grievance, it does not amount to criminal conduct, and therefore they might wish to seek civil recourse and consult a solicitor.

2.7 Fraud prevention advice and current fraud trends can be obtained from online resources e.g. Action Fraud. Action Fraud is mainly a reporting tool for crimes committed in England and Wales, but can be used by the public to report crimes in Scotland. The public have to do this personally. It should not be carried out by Police on their behalf.

2.8 Guidance from the Economic Crime Financial Investigation Unit (ECFIU) depending on an officer's geographic location should always be sought when dealing with fraud or financial crime involving high profile individuals.

2.9 Whilst anyone can be a victim of Fraud, some social groups may be more vulnerable to particular types of fraud and the impact may be greater due to their age / disability (e.g. doorstep / phone / letter scams) or religion (e.g. Hajj related scams). Police officers should in all cases deal with each victim of crime as an individual, taking cognisance of any vulnerability or other issues such as the need to gender match victim and interviewing officer and making appropriate arrangements to facilitate effective communication.

2.10 Officers should make themselves aware of the SOPs relating to Interpreters, Victim Support and Appropriate Adults and for further information and advice contact Specialist Crime Division (SCD) National Safer Communities Equality and Diversity Department **Information has been removed due to its content being exempt in terms of the Freedom of Information (Scotland) Act 2002, Section 30 Prejudice to effective conduct of public affairs** who may be able to provide assistance when dealing with vulnerable members of protected groups.

2.11 Other useful reference sites to be consulted in relation to Frauds include:

- **Police Scotland Website** – (www.scotland.police.uk) this site provides good guidance information and directs victims to report instances to Police Scotland using the 101 number;

- **National Fraud Action** – (www.financialfraudaction.org.uk) this is a Police only website, whereby registered officers can access up to date information and current trends – Free to register and use;

- **Financial Conduct Authority** – (www.fca.org.uk) this site provides up to date information specifically in relation to companies and individuals involved in scams or boiler room schemes;

3. Receipt of Allegation of Fraud

3.1 Any officer receiving a complaint or allegation of fraud should consider the circumstances to satisfy themselves that a crime has occurred.

3.2 Some initial police enquiry may be required to confirm criminal conduct. Guidance is provided within the Crime Recording SOP and the Scottish Crime Recording Standards (SCRS).

3.3 Each case will be assessed on its own merits and may be referred to a specialist department if a specialist response is deemed necessary.

3.4 Investigations may be:

- Conducted locally by uniformed personnel;

  or

- Referred to the Criminal Investigation Department (CID) for consideration of local allocation, in accordance with National Intelligence Model (NIM) level 1 (Crimes affecting a single area or Division);

  or

- In certain cases, further referred to the ECFIU (or equivalent) - NIM levels 2 and 3 (Cross Border crimes affecting more than one Division usually requiring additional resources, or Serious and Organised Crime operating on a National or International scale, that requires a response from dedicated units).

Note: Guidance on NIM can be accessed via the National Intelligence Model Manual.

3.5 If the circumstances suggest NIM level 2 or 3, the enquiry should be referred to the ECFIU for further assessment. The case acceptance process by the ECFIU takes the following criteria into consideration:

- The crime should have been committed within Scotland. If not, it should be referred to the appropriate force for investigation;
- Basic initial investigations should have been conducted, including obtaining a statement from the complainer. This should contain a comprehensive outline of the complaint, along with any relevant documentation;
- If a crime has been established, it should be recorded as per the SCRS (i.e. Initial incident recorded and Crime Report / File raised). A SID log should also be submitted;
- If the matter is being referred to the ECFIU for consideration, it requires to be done formally, accompanied by any relevant documentation, and signed off by a supervisor;
- Upon receipt by the ECFIU, a full case assessment will be conducted. If, after assessment, the matter is not deemed to fall within the remit of the ECFIU, it will be referred back to the submitting officer;

3.6 In some cases, it will not be appropriate for the ECFIU to conduct investigations. This includes:

- Cases where another force has decided not to investigate, other than for geographical reasons;
- Frauds which have already been investigated by the Police or other law enforcement or regulatory agency, unless significant new evidence has come to light;
- Cases where the existence of other proceedings may have a detrimental effect on a criminal investigation and subsequent prosecution.

3.7 Allegations of Fraud are often made directly to the ECFIU by members of the public, external organisations such as financial institutions, and other law enforcement agencies.

3.8 Such reports will be assessed by a supervisor within the ECFIU. Where appropriate, enquiries will be forwarded to the relevant Local Policing Area for allocation and investigation.

3.9 As a guide, the remit of the ECFIU has been provided at Appendix ‘C’. As a general rule, unless the investigation involves geographically widespread enquiries (for example crossing multiple Local Policing Areas), or there is an apparent abuse of professional knowledge (solicitors, accountants, bank employees or other professionals), the enquiry should remain within the Local Policing Area.

3.10 In some cases, the value of the fraud may be a factor, but this is only likely to be considered along with other circumstances. There are a number of sensitive or specialised enquiries including insolvency offences and allegations of public sector corruption. In instances where public sector corruption, bribery or defalcation is reported or suspected, these should be referred to the ECFIU in the first instance, which will have primacy for assessing such matters and determining the most appropriate method of progressing any necessary enquiry, either within Police Scotland or by a public sector partner. Contact should be made with the ECFIU at an early stage. Contact information is contained within Appendix 'D'.

3.11 An initial report of fraud may appear complex. In the absence of a clear investigative strategy, it may not be entirely clear what steps require to be taken. Local Policing personnel are encouraged to contact the ECFIU for advice on their enquiries, however the initial port of call should always be to discuss with their Line Manager or Divisional CID.

3.12 Fraud investigation should be treated like any other crime. The same rules of evidence apply. There may be more documentary evidence than usual, which can be used to corroborate witness evidence, in which case reference should be made to Crown Office and Procurator Fiscal Service (COPFS) Schedule 8 Guidance Manual. Consideration should be given to utilising all investigative tools including specialist services such as handwriting, fingerprints and, where appropriate, other forensic techniques.

3.13 Consideration should be given at the earliest possible stage to the management of productions and potential disclosure issues. A robust system for dealing with productions, especially where there is a high volume of documents involved, will ultimately facilitate interview strategies and police reports to COPFS.

3.14 If the investigation proves complex, early liaison with COPFS is advisable and may prevent wastage of finite resources. Rather than simply seeking direction, the investigating officer should consider the evidence and relay to COPFS what they think is the way forward for the investigation.

3.15 In instances where Private Sector Corruption, Bribery or Defalcation is reported or suspected, this should be referred to the ECFIU who will have primacy for investigating these offences.

3.16 Contact details for local ECFIUs are provided at Appendix 'D'.

3.17 To support police officers and police staff the following flowcharts have been provided:

- Flow chart for Fraudulent Cheque Series (Appendix 'E')
- Flow chart for Fraudulent Card Series (Appendix 'F')
- Flow chart for Fraudulent Card Series Reported by Retailer (Appendix 'G')
- Flow Chart for Allegation of Public Sector Corruption / Bribery (Appendix 'H')
- Flow chart for Allegation of Defalcation (Appendix 'I')

4. Remotely Perpetrated Fraud

4.1 Description

4.1.1 Remotely perpetrated fraud covers numerous MO however all share one main characteristic – there is no physical contact between the victim and the fraudster.

4.1.2 These frauds are most often perpetrated by telephone or email and involve victims being induced to part with money or goods.

4.1.3 Examples of this type of fraud include:

- Advance fee frauds - where victims are persuaded to pay an upfront fee for such things as a loan, to receive a refund of bank charges, taxes or mis-sold insurance, or to receive overseas lottery winnings;
- Share / investment scams (also called boiler room frauds);
- Internet frauds (including auction websites);
- Goods ordered using stolen credit card details;
- Romance frauds.

4.1.4 Although MOs are constantly varying and developing, what makes remotely perpetrated fraud different from other frauds is that the victim and the perpetrator do not meet. However, the usual investigatory principles still apply.

4.2 First Responder

4.2.1 In all circumstances, sufficient details should be noted to establish that a crime has been committed, to raise a Crime Report/File and, if required, to allow an assessment to be carried out.

4.2.2 The locus will often be recorded as the victim's address in the first instance until enquiry reveals where the suspect is based or the point of benefit.

4.2.3 Consult the Crime Recording SOP for assistance in identifying the locus and establishing crime recording requirements.

4.2.4 Information regarding the vulnerability of any victims or repeat offences should be noted.

4.2.5 Certain money transfers can be reversed if funds have not yet been withdrawn. Consideration should be given to either police or the victim immediately contacting the bank or money transfer company for this purpose.

4.2.6 Time-critical evidence such as Closed Circuit Television (CCTV) should be secured at the earliest opportunity, even where enquiry reveals the locus to be elsewhere in the UK. The transfer of crime process may result in such evidence being lost.

4.2.7 Phone numbers, email addresses, IP addresses and screen prints should be obtained at an early stage. It is essential that any relevant technical information be captured and subscribed at an early stage to help progress any enquiry.

4.3 Action in Relation to Boiler Room Frauds

4.3.1 Boiler Room Fraud is a term used when investors are duped into investing in worthless, overpriced or non-existent shares in companies that are of little or no value. In general cold calls are made to potential investors using high pressure sales tactics supported by brochures, documents and, well-constructed websites that apparently legitimise their claims of a high yield of return.

4.3.2 First Contact is likely to be from the victim reporting directly to Police Scotland, from Action Fraud or via Third Party Reporting**.**

- Consideration should be given to briefing staff at Contact Centres in relation to Boiler Room schemes and first response actions for fraud reports.
- Depending on the immediacy of the call (have funds been transferred that day that could be frozen in sending / receiving accounts) review Contact Centre guidance and ensure fit for purpose.

4.3.3 The initial Police attendance should be Uniformed Divisional resources, who should consider if the victim requires support from partner agencies and/or family, and raise a concern report if applicable. A witness statement is required from the victim as well as forensically preserving any documentation including letters, envelopes, brochures, and literature. If available seize the victim's bank statements, emails, telephone records, hand written notes, receipts of cash transactions, deposits (western union) and postal receipts. Ensure all documents are lodged and signed with documentary backing sheets and relevant certification.

4.3.4 Consider securing CCTV evidence if the victim has met with suspects or attended at financial institutions. Staff may assist with enquiries and provide additional witness statements.

4.3.5 In addition, if funds have been transferred that day and the possibility exists of freezing or retrieving the funds, it is essential that guidance be sought from the Divisional Financial Investigation Team, CID or ECFIU, SCD, Gartcosh to enable early communication with the bank or financial institute.

4.3.6 The victim may be targeted by multiple 'Boiler Room' schemes and their details circulated on a 'sucker list'. This can mean that the victim is unable to provide a clear account of transactions or phone calls. Depending on the age and vulnerability of the victim consider recording the victim's statement on audio and visual DVD. This can be crucial in confirming the victim's state of mind and vulnerability and exposing the high pressured sales techniques that have been employed by the Boiler Room scheme. This also highlights the victim's lack of understanding and inability to invest in the product (Gold, Diamonds and Carbon Credits).

4.3.7 A SID log should be submitted at the earliest opportunity and marked FAO National Fraud Intelligence Bureau (NFIB) and ECFIU. Once this information has been collated, early consultation with NFIB, Action Fraud, City of London Police (CoLP) and the ECFIU is advised to determine criminality and jurisdiction. This will establish if a crime report is to be raised.

4.4 Further Lines of Enquiry

4.4.1 SID should be researched for any linked incidents and a SID log submitted at an early stage.

4.4.2 Consider sending an intelligence request to the National Fraud Intelligence Bureau to establish links to other reported crimes or enquiries.

4.4.3 Consider whether seized documents are originals or copies, and whether or not they are business documents. Consult Crown Office and Procurator Fiscal Service (COPFS) Schedule 8 Guidance Manual for details of appropriate certificates of authentication and docquets.

4.4.4 Consider early liaison with PF as outlined in Section 3.

4.4.5 Should advice be required, consult with a supervisor in the first instance and if necessary, contact the ECFIU (or equivalent).

5. Known Suspect

5.1 Description

5.1.1 There are a number of incidents where a crime will be reported and a suspect identified prior to police arrival, for example:

- Embezzlement by member of staff;
- Fraudulent scheme;
- Mortgage fraud;
- Family related fraud.

5.2 First Responder

5.2.1 While these cases may be complex, and the first responder may not ultimately be the enquiry officer, it is expected that an initial statement be noted and relevant enquiries carried out.

5.2.2 Sufficient details should be noted to establish that a crime has been committed, to raise a Crime Record and, if required, to allow an assessment to be carried out

5.2.3 Information regarding the vulnerability of any victims or repeat offences should be noted.

5.2.4 Gather all evidence at the earliest opportunity with particular attention paid to time critical evidence such as CCTV.

5.2.5 Ensure forensic awareness when securing evidence and consider Telecoms data.

5.3 Further Lines of Enquiry

5.3.1 A SID log should be submitted at an early stage.

5.3.2 If enquiry appears protracted or complex, consult a supervisor or specialist units.

5.3.3 Consider search warrants for bank accounts or suspect property addresses.

5.3.4 Consider early liaison with PF as outlined in Section 3.

6. Unknown Suspect where there has been Physical Contact

6.1 Description

6.1.1 Frauds of this nature include:

- Automated Teller Machine (ATM) crime (skimming, card/cash trapping devices);
- Ringing the changes (someone asking for a sum of cash to be changed into notes of a different denomination or currency then intentionally use confusion techniques to defraud);
- Forgery and uttering.

6.2 First Responder

6.2.1 Sufficient details should be noted to establish that a crime has been committed and to raise a Crime Record.

6.2.2 Gather all evidence at the earliest opportunity, in particular time-critical evidence such as CCTV.

6.2.3 Ensure forensic awareness when securing evidence such as skimming devices.

6.2.4 Where bank cards or accounts have potentially been compromised, ensure early contact with the bank to minimise financial loss.

6.2.5 The following additional information should be borne in mind by officers involved in the examination/evidencing of Skimming Devices.

- The device will come in two parts – a card reader/trapper and a camera bar, often the camera bar is missed. They are hard to see and often missed even by ATM engineers.
- A card reader will read the victims card without their knowledge and many cards can be read during the course of the card reader being in place. A card entrapment device simply traps the card as it comes back out the ATM. The victim will often walk away and it is at this point that the suspect then removes the device, recovers the genuine card and camera. Card entrapment has an obvious element of risk as the suspect needs to remain nearby to maintain the card entrapment device.
- Photograph in situ (unless already removed in which case photograph the device locally as in above example).
- Be forensically aware, take the card reader and camera and place it within usual production bags for forensic examination.
- If possible get the ATM unique reference number; this may be of use later when research can be done to identify the genuine cards that have passed through that ATM.

- Be aware, as intelligence has shown that suspect(s) will often be nearby watching their equipment and on occasion have challenged members of the public who discover it.
- Arrest suspect(s) in term of Criminal Justice (Scotland) Act 2016 and raise a crime report for Section 49 (Articles used for fraud) Criminal Justice and Licensing (Scotland) Act 2010.
- Submit an intelligence log using the header “ATM CRIME”.
- Should an arrest be made in respect to the device then the ATM reader can be further examined for data recovery. Financial Fraud Action United Kingdom (FFA UK) have a budget to fund such forensic examinations. However, it should be noted that this funding is **only** available in appropriate cases. For further advice regarding funding applications please contact the Financial Fraud Bureau (FFB) **Information has been removed due to its content being exempt in terms of the Freedom of Information (Scotland) Act 2002, Section 30 Prejudice to effective conduct of public affairs**.

6.3 Further Lines of Enquiry

6.3.1 SID should be researched for any linked incidents and a SID log submitted at an early stage.

6.3.2 Identify whether the crime type is one usually perpetrated by travelling criminals and consider sending out appropriate alerts to other parts of the force area or beyond.

7. Crime in Action

7.1 Description

7.1.1 Examples of this type of fraud include:

- Cashing of stolen or counterfeit cheques;
- Use of stolen or counterfeit credit cards;
- False monetary instruments found in a person’s possession.

7.2 First Responder

7.2.1 Assess sufficiency for detention.

7.2.2 Give consideration to perpetrator having been at other loci.

7.2.3 Forensically preserve physical evidence such as cheques and bank cards.

7.2.4 Gather all evidence at the earliest opportunity, in particular time critical evidence such as CCTV.

7.2.5 Although often reported by banks, ensure steps are being taken to halt any successful payments and minimise financial loss.

7.3 Further Lines of Enquiry

7.3.1 SID should be researched for any linked incidents and a SID log submitted at an early stage.

7.3.2 Where suspects are in possession of apparently legitimate bank cards, bear in mind that stolen account details may be held on the magnetic strip. Consider use of a card reader to verify. ECFIU can assist with this process.

7.3.3 If required, police officers / police staff should take cognisance of the guidance and instruction in the Interpreting and Translating Services SOP, Victim Support SOP and the Appropriate Adults SOP.

7.3.4 Information and advice can also be obtained from Diversity Units - that may be able to provide assistance when dealing with vulnerable members of protected groups.

8. International Enquiries

8.1 Where enquiries in the UK have been exhausted, and it has been identified that the suspect or point of benefit lies abroad, the following points should be taken into consideration when assessing whether or not to instigate international enquiries:

a) The loss incurred, i.e. is it a high value fraud;

b) The likelihood of identifying a culprit or recovering money;

c) The likelihood of prosecution;

d) The risks attached to sending personal details abroad.

8.2 This initial assessment will be made by a Detective Inspector responsible for ECFIU.

8.3 As a general rule, amounts under £10,000 will not merit international enquiries and a detailed SID log should be submitted and disseminated to the National Fraud Intelligence Bureau. There will however be occasions when lower amounts will merit special consideration on a case by case basis.

8.4 Where appropriate, individual cases may be transferred, via Interpol, to the law enforcement authorities in the country with jurisdiction. This decision is a matter for Police Scotland, **not** the National Crime Agency or Interpol.

8.5 If sent to a non-English speaking country, statements must be translated into the language of the receiving country, with Police Scotland meeting the full cost associated with the translations. As such, any decision to translate statements for transfer to the authorities in another country is one for senior management to make.

8.6 Once a decision has been made to transfer an enquiry, the Police Scotland International Liaison Office will facilitate this process.

8.7 It should be noted that in certain circumstances COPFS may decide to prosecute in Scotland despite the offender being elsewhere, i.e. where the victim resides locally. Again, consultation with COPFS may be appropriate to discuss this possibility.

9. Intelligence

9.1 It is vital that intelligence obtained from the investigation of fraud is captured appropriately via the creation of a log on SID. This is of particular significance where a new MO has been identified, or a pattern of activity indicates the emergence or resurgence of a particular trend.

9.2 Furthermore, an up-to-date Scottish Intelligence Database will reduce the amount of duplicated enquiries where suspect details have been reported previously by other victims.

9.3 Intelligence is also used to inform strategic assessments and feed into the national picture.

10. Public Sector Corruption / Bribery / Defalcation

10.1 'Public Sector' is the general term used to refer to employees and officials (elected or appointed) of local and central government, or government departments and other public bodies. Public Sector Corruption applies to any member, officer or servant of a public body who solicits or receives money or other benefit in consideration of improperly influencing the performance of public duties.

10.2 Bribery relates to any function of a public nature, connected with a business, performed in the course of a person's employment or performed on behalf of a company or another body of persons. Therefore, bribery in both the public and private sectors is covered within the meaning of the Bribery Act 2010.

10.3 Defalcation is the term used to refer to acquisitive crimes committed by employees within the unitary authority and would include the misappropriation by fraud, theft or embezzlement of monies, material etc., placed in an employee's charge., Defalcation, is therefore, quite distinct from Public Sector Corruption. Offences of this nature should be referred to the ECFIU in the first instance. Contact information is contained with Appendix 'D'.

Appendix 'A'

List of Associated Legislation

- Section 49 (Articles used for fraud) Criminal Justice and Licensing (Scotland) Act 2010
- Bribery Act 2010

Appendix ‘B’

List of Associated Reference Documents

- Police Scotland Crime Investigation Policy
- Police Scotland Serious and Organised Crime Policy
- Crime Recording SOP
- Scottish Crime Recording Standards (SCRS) – Counting Rules
- National Intelligence Model Manual
- Crown Office and Procurator Fiscal Service (COPFS) Schedule 8 Guidance Manual
- Interpreting and Translating Services SOP
- Victim Support SOP
- Appropriate Adults SOP

Appendix 'C'

Role of Economic Crime Financial Investigation Unit

The role of the Economic Crime Financial Investigation Unit includes the investigation of:

- Major or complex frauds.
- Major embezzlements, including those by professional persons e.g. bank employees, solicitors and accountants.
- Allegations of Public Sector corruption / bribery / defalcation;
- Major enquiries from government departments;
- Commercial crimes against banks and finance houses;
- Fraud, the geographical spread of which makes it impracticable for divisional officers to investigate.

Appendix 'D'

List of Economic Crime / Fraud Contacts

V Division

Economic Crime and Financial
Investigation Unit
Loreburn Street Police Station
Loreburn Street
Dumfries
DG1 1HP

E, J, C and P Divisions

Economic Crime and Financial
Investigation Unit
Fettes Police Station
Fettes Avenue
Edinburgh
EH4 1RB

G, K, L, Q, and U Divisions

Economic Crime Financial
Investigation Unit (West)
OCCTU
Specialist Crime Division
Scottish Crime Campus
Gartcosh.
G69 8AE

N Division

Economic Crime and Financial
Investigation Unit
Inverness Police Station
Old Perth Road
Inverness
IV2 3SY

A Division

Economic Crime and Financial
Investigation Unit
Aberdeen Police Station
Site 21,
Badentoy Avenue
Portlethen
Aberdeen
AB12 4YB

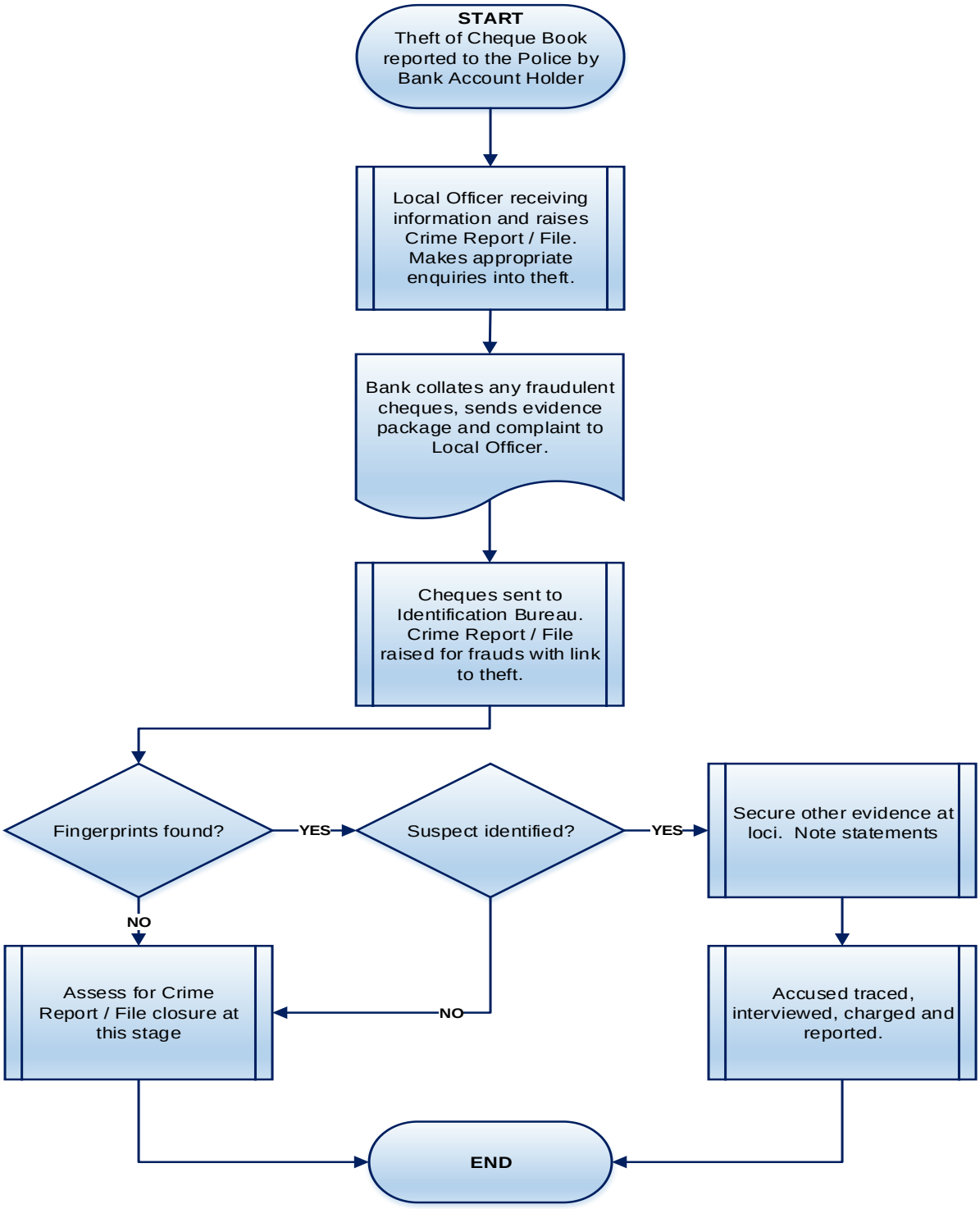
D Division

Economic Crime and Financial
Investigation Unit
Dundee Police Station
PO Box 59,
West Bell Street
Dundee
DD1 9JU

Information has been removed due to its content being exempt in terms of the Freedom of Information (Scotland) Act 2002, Section 30 Prejudice to effective conduct of public affairs

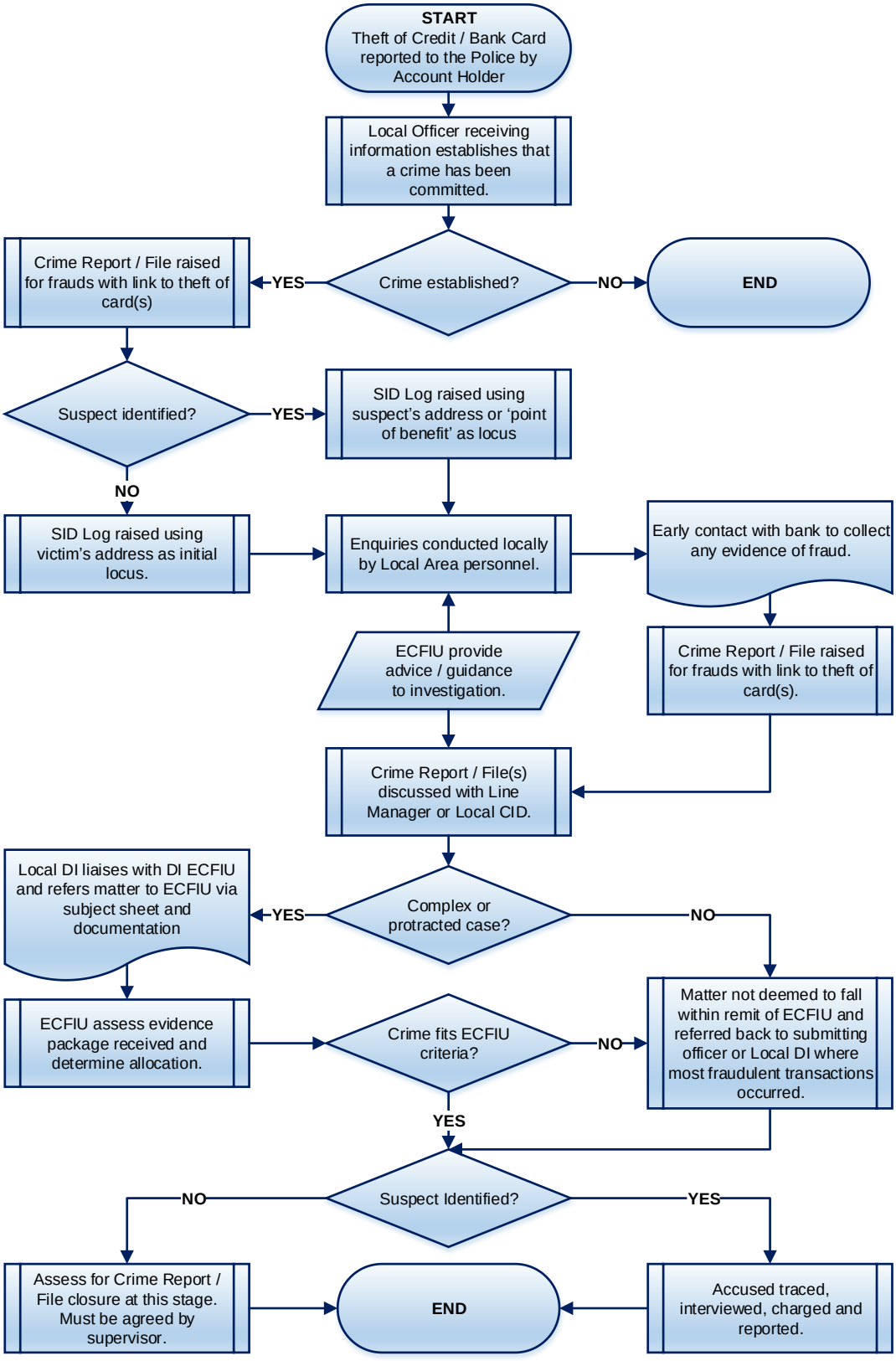
Appendix ‘E’

Flow Chart for Fraudulent Cheque Series



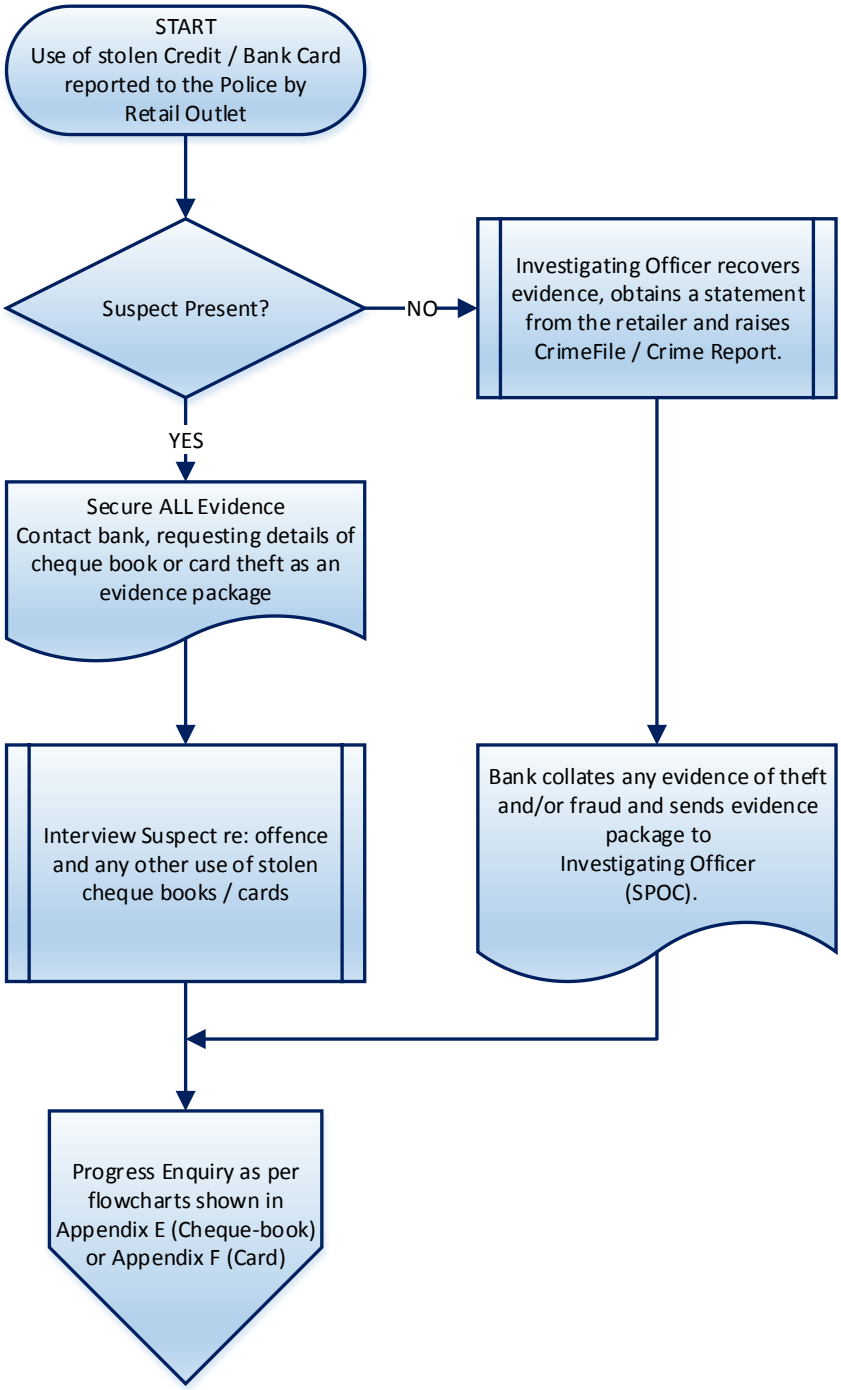
Appendix 'F'

Flow Chart for Fraudulent Card Series



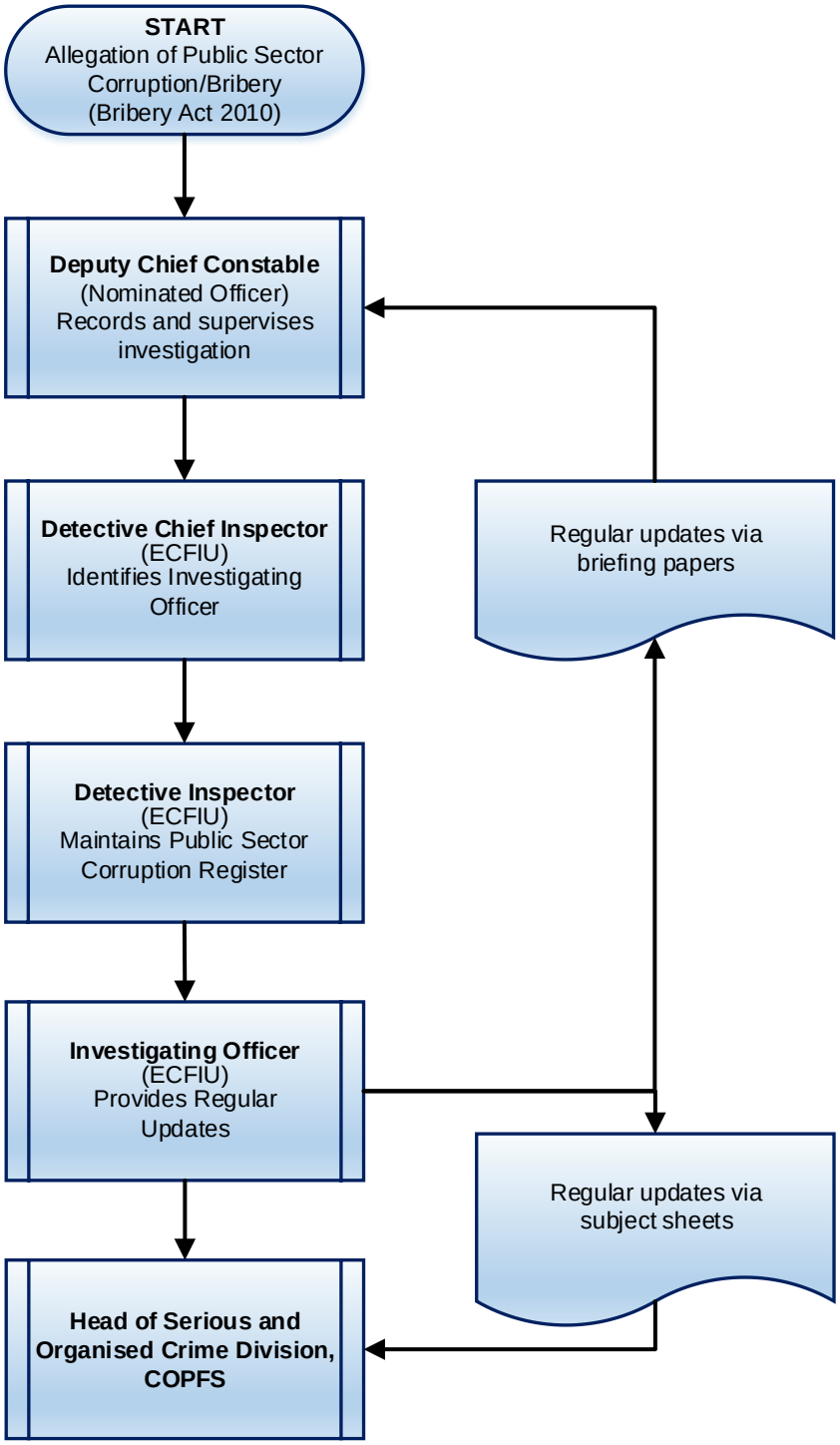
Appendix ‘G’

Flow Chart for Fraudulent Card Series Reported by Retailer



Appendix 'H'

Flow Chart for Allegation of Public Sector Corruption / Bribery



Appendix 'I'

Flow Chart for Allegation of Defalcation