Fraud
Response Plan

Contents

1 Reporting fraud suspicions

1.1 Initial guidance if you suspect a fraud.

A fraud may be uncovered in a variety of ways, from your own observations, someone from inside or outside blowing the whistle, ongoing controls throwing up a discrepancy, internal or external audit discovering a problem, or external regulators and inspectors finding something. It is important for you to know how to deal with your suspicions.

Things to do:

Stay calm – remember you are a witness not a complainant

Write down your concerns immediately – make a note of all relevant details such as what was said in phone or other conversations, the date, the time and the names of anyone involved

Consider the possible risks and outcomes of any action you take

Make sure your suspicion is supported by facts, don't just allege.

Things not to do:

Do not become a private detective and personally conduct an investigation or interviews

Do not approach the person involved (this may lead to him/her destroying evidence)

Do not discuss your suspicions or case facts with anyone other than those persons referred to below unless specifically asked to do so by them

Do not use the process to pursue a personal grievance

Some things to remember:

You may be mistaken or there may be an innocent or good explanation – this will come out in the investigation

The process may be complex and you may not be thanked immediately and the situation may lead to a period of disquiet or distrust in the organisation despite your having acted in good faith

1.2 Reporting your suspicions.

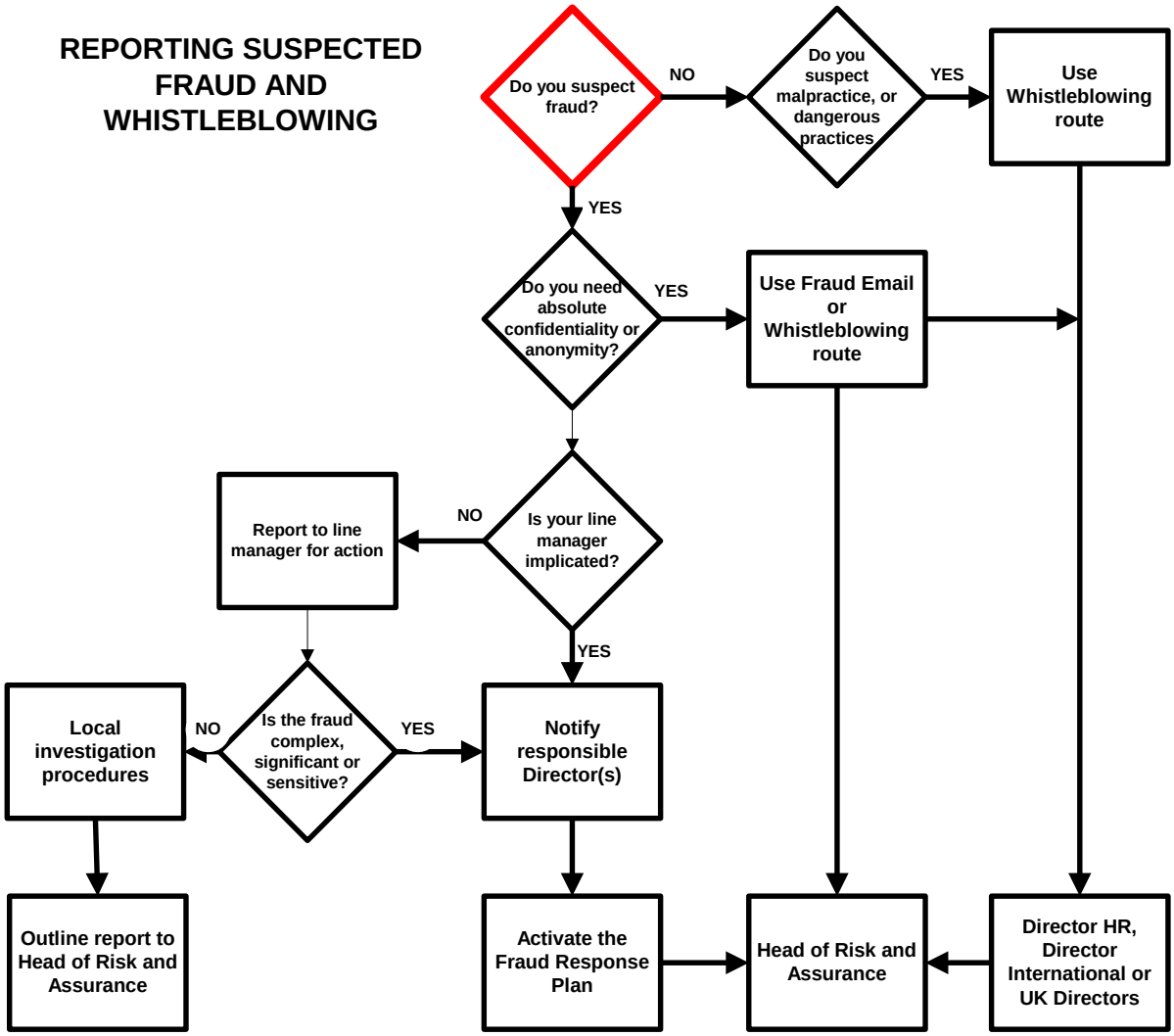
The following reporting lines are to be used regardless of the potential magnitude of the fraud, which it would be difficult to quantify at an early stage. Report your suspicions as below:

- **Your line manager.**
  Generally this is your first port of call. Fraud prevention is their responsibility in particular. They will know the systems, the people, what is at risk. They should know whom to bring in.
- **A more senior manager or your Director.**
  If you think your manager might be involved in the fraud or if you feel they have wrongly dismissed your concerns, then you should go to a more senior manager or your Director.
- **Fraud reporting email / internet**
  If you want to be assured of absolute confidentiality or wish to remain anonymous, you can report to the Head of Risk and Assurance using fraud@redcross.org.uk.

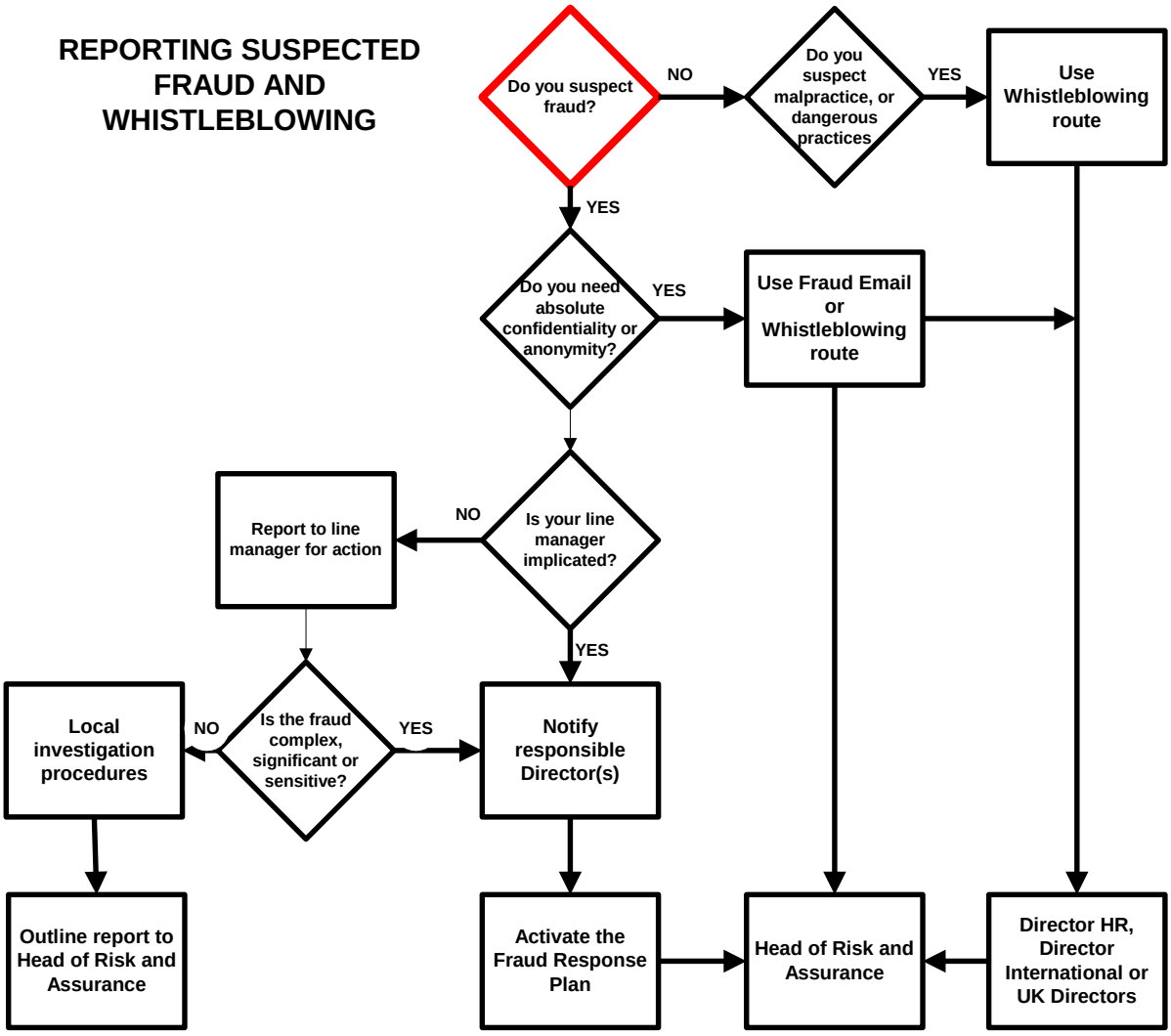
Whistleblowing
The Whistleblowing Policy on the intranet provides advice on reporting criminal acts (such as fraud). You should write to the Director HR, Director International or any UK Director. Provided reports are made in good faith, you are protected by the British Red Cross and the law against retribution, harassment or victimisation and your confidentiality will be preserved.

1.3 Guidance for line managers on receiving a report of fraud:

- Listen to the concerns of your staff and treat every report you receive seriously and sensitively. Make sure that all staff concerned are given a fair hearing.
- You should reassure your staff that they will not suffer because they have told you of their suspicions.
- Get as much information as possible from the member of staff. Do not interfere with any evidence and make sure it is kept in a safe place.
- Request the member of staff to keep the matter fully confidential in order that senior management are given time to investigate the matter without alerting the suspected/alleged perpetrator
- If you suspect the fraud involves another department then you should notify a senior manager in that department, or the Director for further action in accordance with this policy.
- If the suspected fraud is small, simple and routine (such as a shop fraud) and you feel capable of handling the investigation yourself or there are standard procedures to follow, then this is an option. You should still refer to this Policy and the Fraud Response Plan for advice and the outcome, should be reported to the responsible Director and the Head of Risk and Assurance regardless of the result.
- If you believe the suspected fraud to be complex, significant, sensitive (e.g. the reputation of the British Red Cross is at stake) or implicates a senior member of management, then do not carry out an investigation yourself – this could hinder proper investigation and any criminal enquiry. Report the matter immediately to senior management, your Director and the Head of Risk and Assurance or other person with responsibility for investigating fraud allegations. They will decide on activation of the Fraud Response Plan.


REPORTING SUSPECTED FRAUD AND WHISTLEBLOWING
Do you suspect fraud?
NO
Do you suspect malpractice, or dangerous practices
YES
Use Whistleblowing route
YES
Do you need absolute confidentiality or anonymity?
YES
Use Fraud Email or Whistleblowing route
NO
Is your line manager implicated?
Report to line manager for action
YES
Local investigation procedures
NO
Is the fraud complex, significant or sensitive?
YES
Notify responsible Director(s)
Outline report to Head of Risk and Assurance
Activate the Fraud Response Plan
Head of Risk and Assurance
Director HR, Director International or UK Directors

2 Stages prior to fraud response plan



3 Fraud Response Plan

3.1 Introduction

It is important that managers and others know what to do in the event of a fraud so that they can act without delay. The Fraud Policy covers the action required when fraud is suspected and to whom the fraud or suspicion should be reported. The Fraud Response Plan is a guide to how and by whom the fraud suspicion will then be investigated, reported and closed.

The Fraud Response Plan provides an outline of many of the areas that will need to be considered when investigating a large and complex fraud. For smaller less complex frauds, there will be parts of the plan that will not be applicable. It is however important to keep an open mind and consider whether a small fraud is concealing a much larger fraud.

	Date	Comment
3.2 Immediate action		
All cases that reach this stage must be notified to: • the Director responsible for the area of the suspected fraud • the Head of Risk and Assurance • the Director of Finance and Resources		
The suspected fraud must be recorded in: • the Fraud Register, updated as the investigation progresses (see appendix) • Special Payments, losses and compensations register depending on outcome of investigation		
A fraud investigation file should be created and this checklist inserted.		
3.3 Meeting of the Fraud Response Team		
The responsible Director, Head of Risk and Assurance or the Director of Finance must arrange for the creation and meeting of a Fraud Response Team as soon as possible. Membership of the Team may vary depending on initial indications of the severity of the suspected fraud but may include: • the Director responsible for the area of the suspected fraud • the Head of Risk and Assurance • the Director of Finance and Resources • Director of HR For smaller, less complex frauds, it may not be appropriate to establish a full Fraud Response Team but the Head of Risk and Assurance should always be a member and should be kept informed of progress at all stages of the investigation.		
Membership of the Fraud Response Team should be established as part of agreeing and signing off the Fraud Response Plan.		

	Date	Comment
The Fraud Response Team should quickly determine the following: • whether an investigation is necessary • who will lead the investigation (The person chosen to lead the investigation should be appropriately experienced and independent of the activity affected by the alleged fraud). • any necessary additional resource to support the investigation • any immediate need for police involvement • any additional support requirements (e.g. IT facilities, a secure room, secure fax and phone facilities, administrative support etc) • any immediate need for legal advice • any immediate need for external, technical advice or support (e.g. forensics) • any immediate need to establish a PR/media strategy for dealing with the case (both internally and externally) • any immediate need to suspend staff; conduct searches and remove staff access (e.g. to files, buildings, computers/systems etc) • any immediate need to report the potential fraud externally (e.g. Charity Commission, external auditors, funders/donors, tax authorities etc). • whether the fraud is suspected to approach the insurance excess (currently £50,000) and therefore the insurers need to be informed. • Whether the chair of the Audit Committee should be informed. • a timetable for the lead investigator to report back progress on the investigation.		
The objectives of the investigation should be documented and approved by the Fraud Response Team at the outset. Likely objectives would be to: • identify the culprit(s) • establish the facts surrounding the fraud and ascertain total losses • remove the threat of further losses. (Note: in some exceptional cases it may be necessary to allow further losses, in order to gain additional evidence and increase the chances of successful criminal, civil, or disciplinary action. This should normally only be allowed under police guidance). • obtain sufficient evidence for successful disciplinary, criminal, or civil action		
Certain action may need to take place immediately to prevent further losses. The Head of Human Resources should lead on any decisions and action regarding staff suspensions and removal of access to files, systems and offices.		
The date of the next meeting and review of the first investigation progress report should be agreed. The Fraud Response Team should arrange to meet on a regular basis, to oversee progress of the investigation and to take major decisions relating to the case.		
3.4 The Lead Investigator's plan		
The lead investigator should prepare an investigation plan, which should be submitted to the Fraud Response Team for approval.		
The Plan should be fairly short term, as developments in the investigation will invariably result in changes. It should show clearly what work/tasks need to be completed, by whom and when.		

	Date	Comment
The Plan may cover some or all of the following: • identification and recording of the persons involved and facts of the case • handling internal and external communications • actions to prevent further losses • actions to secure evidence. Normally, evidence should be secured in a way that will be least likely to alert the suspect(s) or others • liaison with Human Resources and dealing with employees under suspicion • interviews to be conducted • timetables for involving the police or other external experts • analysis of evidence • internal reporting (e.g. to Management Team, to Audit Committee, etc) • reporting to regulatory/government bodies • target dates for reporting back to the Fraud Response Team		
3.5 Communications during and after the investigation		
The effectiveness of the Plan depends on good quality communication at all stages.		
Internal communications • Investigators and managers need to ensure that everyone with a need to know is kept suitably briefed throughout the investigation and at the reporting, acting on findings and debriefing stages. Communication with any person(s) about whom concerns are raised needs to be conducted in accordance with the organisation's HR policies. The person who raised concerns should be kept up to date, with due regard to confidentiality. • There will always be a balance to be struck between communication and confidentiality therefore those persons or categories of persons who need to know should be clearly identified at each stage of the Plan, so that assurances on confidentiality can be given where required		
External communications • Third parties who may need to be alerted or informed might include the police, regulatory authorities, insurers, legal advisors, external auditors and the Charity Commission. The Plan should make clear who is mandated to communicate with these third parties, and under what circumstances. • British Red Cross is prepared for the fact that frauds may attract media attention and the Plan should identify which employee is mandated to deal with the press and what action any other staff contacted by the press should take. The current media communication channels and procedures should be used where possible		
Inappropriate communication The Plan should make clear any form of communication that is considered inappropriate, for example: • discussing the case outside the British Red Cross • confrontation between the person reporting the fraud and the suspected perpetrator(s). (Note that the Whistle blowing Policy provides assurances for the safety and confidentiality of the person making the report)		

	Date	Comment
3.6 Securing evidence		
• In securing and handling evidence it should be assumed that all evidence may need to be presented in court and should therefore be treated accordingly. (Even if criminal or civil action is not planned, it is sensible to adopt this approach). • Normally, all evidence should be kept securely under lock and key, with access limited to those working on the investigation. If necessary, locks to secure rooms should be changed. A record should be maintained of anyone handling evidence. • Evidence such as computer data, transferable media, videotape etc, should only be handled by suitably trained and skilled personnel. Where there is any doubt, professional/police advice should be sought • Where evidence, or other relevant information, is to be shared with another body, careful consideration should be given to any data protection (confidentiality) requirements. Where there is any doubt, expert advice should be sought. • Evidence can take different forms and will need to be handled in different ways.		
Original Documents • handle as little as possible • put in protective folder and label the folder • do not mark in any way • assign responsibility to one person for keeping the documents • keep a clear record of how and where the documents were obtained • keep a record of anyone who subsequently handles the documents		
Computer Held Data/Transferable Media • keep secured in an appropriate environment • data should only be retrieved from computers by those who are technically qualified		
Photocopied Documents • in some cases it may be preferable or necessary to leave original documents in situ and take photocopies for further analysis and investigation • photocopies should be clearly marked as such • photocopies should be signed and dated, and certified as a true copy of the original		
Video/DVD/CD Rom Evidence • keep secured in an appropriate environment (e.g. protective bag) • videos should not be viewed until technical and legal advice is sought (i.e. so that they can be treated in accordance with the rules of evidence).		
External evidence • There are potential external sources from which evidence or information to support an investigation can be obtained, such as the tax authorities, supplier records, government registers of companies, donor records etc.		

	Date	Comment
3.7 Employees under suspicion		
• It should always be remembered that an allegation of fraud may be unfounded and in order to respect the employee and ensure good working relations after an investigation, any action taken, such as suspension, and interviewing should be handled very carefully. • Suspension from work is an opportunity to protect both the employer and employee, providing the necessary space and opportunity to plan the investigation, investigate the facts and speak to other staff without the employee being present. It should be made clear that suspension is not a judgement. • The key factors in deciding to suspend staff will normally be prevention of further losses and removal or destruction of evidence. In some cases, it may be preferable to not suspend even at the risk of further losses (e.g. to gather further evidence). • Any employees under suspicion who are allowed to remain at work should be closely monitored. This may include: physical surveillance of movements, monitoring of IT usage, monitoring of telephone, email and internet usage etc. (Note: it is advisable to seek legal advice regarding the use of surveillance techniques, to ensure compliance with local laws such as the Regulation of Investigatory Powers Act in the UK). • Other matters to consider include: • a review of staff records (e.g. to check references, employment history, qualifications etc, but with due regard to any data confidentiality / protection requirements) o searching the suspects work area; desk, cabinets, files, computer etc o restricting access by the suspect to files, computers etc.		
3.8 Interviews/statements		
• When interviewing employees under suspicion it must be made clear whether it is a formal interview or an informal discussion. It should be explained that you have no pre-set view, the suspicion should be outlined and the employee given adequate time to respond. • If it is decided that formal questioning is needed because involvement in a criminal offence is suspected, then the interview should be conducted in accordance with the principles of the UK Police and Criminal Evidence Act (PACE). Guidelines can be found on the Home Office Website • PACE provides protection for the individual and ensures that any evidence collected through interviews, (including the taking of statements) can be presented in court whether or not such interviews are being carried out under caution. PACE covers such rights as the right to silence, to legal advice, not to be held incommunicado, to accurate recording and protection against evidence obtained through oppression. If necessary, seek legal/police advice. (Where local legislation is more applicable then this should be referred to and followed). • Interviews should only be carried out with the approval of senior management/the Fraud Response Team. • Early consideration should be given to police involvement, or consultation. • There are strict rules relating to tape recorded interviews and investigators must be suitably skilled and experienced, where these are used. • Ideally, statements should be taken from witnesses using their own words. The witness must be happy to sign the resulting document as a true record – the witness can be given a copy of the statement if desired. • It is very important to keep contemporaneous notes on file, in the event that they are needed for future reference (e.g. court, tribunal, disciplinary hearing). Such notes should always show: date of interview; time started; time finished; and, be signed and dated by the interviewer.		

	Date	Comment
3.9 Police involvement		
• At some point a decision will need to be made as to whether the case is reported to the police. It is British Red Cross policy to automatically report all frauds and thefts to the police, but there needs to be an element of realism as to the likely extent of police involvement. For large-scale frauds, it may be appropriate to ask the police to attend meetings of the Fraud Response Team. • The lead investigator should prepare an "Evidence Pack" that can be handed to the police at the time the fraud is reported. The Evidence Pack should include a summary of the fraud, highlighting (where known) the amount, the modus operandi, and the location, and including photocopies of key supporting documents and contact details of the person leading the investigation. Remember to keep a photocopy of everything that is handed to the police. • All contact with the police should be channelled through one person (i.e. the person leading the investigation). A record should be maintained of all contacts with the police, the details of the officers, and the crime reference number. • The Police have knowledge of similar cases of fraud and their advice should be sought regarding measures to prevent further losses or future incidents.		
3.10 Prevention of Further Losses		
• Once actual or potential losses have been identified it is important that effective and timely action is taken to prevent further losses. It may however be decided that a better standard of evidence can be obtained by allowing limited further losses. • The person in charge of the investigation should, at an early stage in the process, complete a preliminary assessment of the potential for further losses and how best to prevent them. He should make recommendations to senior management as to what if any immediate actions are necessary. • Actions taken at an early stage may have to be circumspect so as not to alert suspects who have yet to be suspended or cautioned. It may also be important not to lose or compromise the forensic value of data by precipitate action. It may nevertheless be necessary to act quickly e.g. to stop salary payments to suspects who are to be dismissed. • As the investigation continues, and more information emerges, further recommendations for action may be needed. At the end of the investigation Risk and Assurance should review all the actions taken to prevent further losses and to report on this in the Review of Findings.		
3.11 Recovery of Losses s		
• Once the identity of the perpetrator (s) and the size of the fraud has been determined management must consider whether or not any of the loss can be recovered and take any further action that is necessary. This may require advice from the Insurers.		
Reimbursement offered during the investigation • An individual may, in the course of an investigation, offer to repay the amount that has been obtained improperly. The person in charge of the investigation should neither solicit nor accept such an offer (as it may be construed as having been obtained under duress). The lead investigator should record any offer made and refer the individual to the relevant Manager or Head of Human Resources.		
Reimbursement offered during disciplinary or legal proceedings • If an offer of restitution is made while disciplinary or legal proceedings are still under way, management must seek legal advice before such an offer is accepted.		
Reimbursement after completion of disciplinary proceedings • Where a member of staff is to be dismissed, the manager should consider recovery of amounts due from any outstanding salary or expense payments. It will be necessary to take legal advice about the right to do this as it is unlikely to be clear in the employee's contract of employment.		

	Date	Comment
Court Order • Where a criminal case is taken against an individual a formal claim for restitution (where the court orders the defendant to give up gains) should be made through the Police. Any monies due will be recovered via a Court Order.		
Civil Action • Funds lost due to fraud can be recovered from the perpetrator by suing them for damages in a civil court. The level of proof required in civil cases is lower than that required in criminal cases and management may regard a civil action as a more effective use of their time than trying to persuade the Police to investigate and the courts to prosecute. If this approach is successful the perpetrator will also have to pay British Red Cross's legal costs. • A civil action can still be brought even if a criminal prosecution has failed. If a criminal prosecution is successful a civil action may be necessary to force the person convicted to repay the sums stolen. • It is important to remember that the person being sued may be unable to make the repayment. In situations in which repayment is unlikely senior management approval should be obtained before additional legal costs are incurred		
Commercial Negotiation • Where the fraud has been committed by the employee of a contractor or supplier all or part of the loss may be recoverable from the business concerned. It may be possible to reach an agreement that the loss can be deducted from any outstanding debts or that additional goods/services will be supplied free of charge. • Third parties may want to agree a negotiated settlement in order to retain the goodwill of their customer and/or to avoid damaging publicity and legal costs. They may subsequently be able to recover these costs from their employees or their insurers		
Insurance • The insurers should be informed as soon as a suspicion is raised. In certain circumstances it may be possible, to make a claim against the insurers. The person who led the investigation should provide the insurers with any information that; is required to substantiate a claim, or to support an attempt by the insurers to secure recovery from the perpetrator.		

	Date	Comment
3.12 Administration		
• Careful administration of the investigation is of vital importance. A disordered investigation, without clear records and logs of events, communications, key dates etc, will cause problems at any court hearing, employment tribunal, or disciplinary panel. • Maintain a chronological record of all events on a main file. This should include all correspondence, telephone calls and emails made and received, interviews, visits, tests/checks undertaken etc. • Maintain a list of all contacts (e.g. internal, police, charity commission, lawyer, donors/funders, peer organisations, government bodies, technical advisers). • Maintain a list of emergency contact numbers and ensure that this is shared with all those on the list (e.g. Chief Executive, Director of Human Resources, Head of Risk and Assurance). • Maintain a log of anyone who handles evidence obtained, including the police. • Consider whether there is a need for: dedicated administrative support; dedicated phone and email address; secure fax machine; secure room etc. • Do not keep any unnecessary records or copies. Carefully shred any papers that are not needed (e.g. extra copies of progress reports). • Establish internal and external communication protocols. Discourage the use of email to communicate sensitive information; avoid internal mail and hand deliver highly confidential information, opting for double-enveloped post for less sensitive information. Where email is used for communication, consider entering subject names that have no direct link to the investigation. • Provide update reports as appropriate (e.g. Fraud Response Team, Audit Committee, regulatory bodies, external auditors).		
3.13 Reporting		
• Every investigation of suspected fraud or financial irregularity should result in a report written by the person who led the investigation. This should be done regardless of whether any members of staff are dismissed or prosecutions made. • The report will record, the scale of the fraud, when and how it was perpetrated and by whom. In addition the report will record; what action has been taken against the perpetrator, the actions to prevent further similar losses and to recover what has been lost. It will also usually be pertinent to note how the fraud was detected and whether or not existing controls were effective. • The report will be issued to the Chief Executive, the Director of Finance, the relevant Director, the Head of Risk and Assurance and the Trustee who chairs the Audit Committee and is responsible for Risk and Assurance. A copy should also be made available to the External Auditors. • Since the report may be used internally for disciplinary hearings or externally for civil or criminal proceedings, conclusions and opinions should be substantiated by evidence and any defamatory statements should be avoided. • It is important to strictly limit the distribution of the report. Copies will not be provided automatically to suspects or their representatives. If a disciplinary hearing takes place the individual and their representative may be entitled to receive a copy subject to obtaining legal advice.		

	Date	Comment
3.14 Review, communication and action on Findings		
Review of findings • The findings reported by the person in charge of the investigation should be reviewed by relevant managers and in particular the lessons learned to avoid future frauds. If the fraud was significant the findings should be discussed by the Audit Committee. • Senior Managers should satisfy themselves that, so far as is practically possible, a similar fraud could not occur again and /or the amount of potential loss has been minimised, the perpetrators have been properly dealt with and recovery has been pursued robustly. • Managers and supervisors should be disciplined if they have not properly enforced existing controls and procedures.		
Communicating outcomes • Responsibility for communicating findings and actions to those involved and others who need to know should be set out in the Plan. The British Red Cross will hold a debriefing once outcomes have been finalised, to ensure that proper closure has been achieved. • It may be necessary to manage the expectations of the person who raised concerns. The Whistle blowing Policy provides guidance on what may be communicated		
Action on Findings • Any actions arising from the final report should be allocated to named individuals with appropriate due dates for completion. • The final details of the fraud should be added to the entry in the British Red Cross Fraud / Special Payments, Losses and Compensations register (see the section "Immediate Action" above). • On an annual basis the monetary value of funds lost due to fraud must be reported to the Charity Commission.		
3.15 Closure		

Communication that the case has been closed
• It is important that any decision to close the case is clearly documented and communicated to those involved.
• The case may be closed for a number of reasons, including
  ○ All action points that arose from the final report have been completed
  ○ The Fraud Response Team decides there is insufficient evidence to support the allegations
  ○ British Red Cross does not wish to incur further costs investigating the case
• The decision to close the case and the reason for doing so should be documented by the person leading the investigation and should be added to the investigation file.		

Archiving • All documents associated with the investigation should be archived in a secure location with adequately restricted access. • Any redundant documents and papers, or duplicate copies, should be carefully shredded.		

4 Appendix Legal definitions of fraud

The Fraud Act 2006 (UK): The Fraud Act 2006 received Royal Assent on 8 November 2006 and came into into effect on 15 January 2007. The Act creates a new general offence of fraud with three ways of committing it:

- Fraud by false representation
- Fraud by failing to disclose information, and
- Fraud by abuse of position

It also creates new offences:

Obtaining services dishonestly

Possessing, making and supplying articles for use in frauds

Fraudulent trading applicable to non-corporate traders.

Fraud Act 2006

2006 CHAPTER 35

An Act to make provision for, and in connection with, criminal liability for fraud and obtaining services dishonestly. [8th November 2006]

BE IT ENACTED by the Queen's most Excellent Majesty, by and with the advice and consent of the Lords Spiritual and Temporal, and Commons, in this present Parliament assembled, and by the authority of the same, as follows:—

Fraud

1 Fraud

(1) A person is guilty of fraud if he is in breach of any of the sections listed in subsection (2) (which provide for different ways of committing the offence).

(2) The sections are—

(a) section 2 (fraud by false representation),

(b) section 3 (fraud by failing to disclose information), and

(c) section 4 (fraud by abuse of position).

Money Laundering - the Proceeds of Crime Act 2002 and Money Laundering Act 2003

Money laundering is the process by which the proceeds of crime are converted into assets, which appear to have a legitimate origin. (see appendix, examples of fraud).

Terrorism Act 2000

Under the Terrorism Act 2000 the assets of charities can be frozen if they are shown to have funded terrorists. (see appendix, examples of fraud).

5 Appendix Examples of fraud

Theft: the illegal taking of someone else's property without that person's freely-given consent. Apart from the obvious theft of British Red Cross physical assets such as computers, shop stock and money, it includes:

- Misappropriation of funds
- Misuse of assets, including cash, stock and other assets, for example “borrowing” petty cash, use of photocopiers for private purposes
- Theft from a client or supplier
- Theft of intellectual property (e.g. unauthorised use of the British Red Cross name/logo, theft of product / software designs and client data.

Bribery: this implies a sum or gift given that alters the behavior of the person in ways not consistent with the duties of that person. It includes offering, giving, receiving or soliciting any item of value in order to influence an action.

Corruption: this is a general concept describing any organized, interdependent system in which part of the system is either not performing duties it was originally intended to, or performing them in an improper way, to the detriment of the system's original purpose.

Deception: to intentionally distort the truth in order to mislead others. It would include obtaining property, services or pecuniary advantage by deception or evading liability. Deceptions include:

- misrepresentation of qualifications to obtain employment
- obtaining services dishonestly via technology e.g. where a credit card that has been improperly obtained is used to obtain services from the internet, or any other situation where false information is provided to a machine
- possessing, making and supplying articles for use in fraud via technology e.g. computer programs designed to generate credit card details that are then used to commit or facilitate fraud
- undeclared and unauthorized private and consultative work
- money laundering (see below).
- Providing misleading information to donors in order to obtain funds, such as overstating activity (note that this is an example of a fraud for the benefit of the British Red Cross rather than to its detriment).

Forgery: this is the making or adapting objects or documents with the desire to deceive.

Extortion: this occurs when a person obtains money or property from another through coercion or intimidation.

Embezzlement: this is the fraudulent appropriation by a person to their own use of property or money entrusted to that person's care but owned by someone else.

False Accounting: this is dishonestly destroying, defacing, concealing or falsifying any account, record or document required for any accounting purpose, with a view to personal gain or gain for another, or with intent to cause loss to another or furnishing information which is or may be misleading, false or deceptive. It includes:

- Manipulation or misreporting of financial information
- Fraudulent completion of official documents (e.g. VAT receipts)

Conspiracy: this is an agreement between two or more persons to break the law at some time in the future. It includes breaches of regulations.

Collusion: the term "collusion" covers any case in which someone incites, instigates, aids and abets, conspires or attempts to commit any of the crimes of fraud.

Money laundering: this is the term used to describe the ways in which criminals process illegal or 'dirty' money derived from the proceeds of any illegal activity (e.g. the proceeds of drug dealing, human trafficking, fraud, theft, tax evasion) through a succession of transactions and deals until the original source of such funds has been obscured and the money take on an appearance of legitimate or 'clean' funds.

There are three internationally accepted phases to money laundering:

- **Placement** – this involves the first stage at which funds from the proceeds of crime are introduced into the financial system or used to purchase goods. This is the time at which the funds are most easily detected as being from a criminal source. Such 'dirty money' will often be in the form of cash or negotiable instruments such as travelers cheques.

- **Layering** – this is where the funds pass through a number of transactions in order to obscure the origin of the proceeds. These transactions may involve entities such as companies and trusts (often offshore).

- **Integration** – this is when the funds are available via a legitimate source and allow the criminal to enjoy access to the funds again, with little fear of the funds being detected as being from a fraudulent source.

There are three main areas where by BRC may become exposed:

1. A charity may be formed with the intention to undertake some form of criminal activity (which may include tax evasion). These charities are likely to be small or have a short life cycle since their affairs will be less scrutinised however they may well attempt to gain partnership status with BRC.

2. BRC may benefit from crime by receiving a grant or completing a contract with money which would fall under the definition of bribery.

3. BRC may be specifically targeted for money laundering. Staff and volunteers should look out for gifts that were subsequently asked to be repaid as though they were loans, or gifts with unusual conditions such as a certain amount being passed on to a particular destination, loans being made in one currency and then repaid in another, or loans made in cash and due to be repaid in cheque

6 Appendix Terrorist Financing (Terrorism Act 2000)

Under the Terrorism Act 2000 the assets of charities can be frozen if they are shown to have funded terrorists. BRC staff should therefore be aware of terrorist organisations posing as legitimate entities which can conceal the diversion of funds to terrorist organisations.

Example 1:

An employee working for an International Aid organisation in a war torn region used his occupation to support the on-going activities of a known terrorist organisation. The employee had secretly made contact with those who would smuggle weapons in that region

and used his position as a cover whilst he arranged the purchase and export of weapons to the terrorist organisation.

Example 2:

An employee working for a charity obtained surplus funds from Head Office to fund terrorism by padding the number of orphans it had claimed to care for by providing the names of orphans who were either dead or did not exist. Funds were then diverted to local terrorist organisations. The office also employed members of the terrorist organisations and facilitated their travel.

7 Appendix Examples of controls to prevent and detect fraud

- thorough recruitment procedures
- physical security of assets
- clear organisation of responsibilities and reporting lines
- adequate staffing levels
- supervision and checking of output
- separation of duties to ensure that key functions and controls are not performed by the same member of staff
- rotation of staff
- random spot checks by managers
- complete and secure audit trails
- performance monitoring by management
- budgetary and other financial reports
- reviews by independent bodies such as audit

8 Appendix Warning signs for fraud

There are warning signs that can indicate a fraud may be taking place, these can include:

- staff under stress without a high workload
- reluctance to take annual leave
- being first to arrive in the morning and last to leave in the evening
- refusal of promotion
- unexplained wealth
- sudden change of lifestyle
- suppliers/ contractors who insist on only dealing with one staff member
- a risk taker or rule breaker
- disgruntled at work / not supportive of organizations mission

Fraud Indicators can include:

- staff exhibiting unusual behavior (see list above)
- missing key documents (invoices/ contracts)
- inadequate or no segregation of duties
- documentation which is photocopied or missing key information
- missing expenditure vouchers
- excessive variations to budgets / contracts
- bank and ledger reconciliations not regularly preformed and cannot be balanced
- numerous adjustments or exceptions
- overdue pay or expense advances
- duplicate payments
- ghost employees on payroll
- large payments to individuals
- crisis management coupled with a pressured work environment
- lowest tenders or quotes passed over without adequate explanation
- single vendors

- climate of fear / low staff morale
- consistent failure to implement key controls
- management frequently overriding controls

9 Appendix Fraud Register

The Fraud Register contains the following headings:

- Case number
- Date of reporting
- Location of incident(s)
- Nature of alleged incident
- Key persons involved
- Time period over which the incident(s) occurred
- Value (estimated or actual) associated
- References to documentary and other evidence sought or acquired
- Control weaknesses identified
- Recommendations for improvement / further action identified
- Responsibilities and time frames for action