



APPENDIX A
(CFO/158/07)

Merseyside Fire & Rescue Service Fraud Response Plan

Contents

	Page
Introduction and Scope	2
Part 1 - For all staff	3
• Who to inform	3
• What NOT to do	4
• Points to consider	4
Part 2 – For Managers	5
Appendix A	15
Appendix B	16

Introduction and Scope

This document is intended to address Merseyside Fire and Rescue Service's (MFRS) response to any actual or suspected fraud or financial irregularity committed against MFRS involving any employees or third parties (eg general public, contractors, partnership staff and claimants).

Part 1 of the document is for all MFRS employees and is designed to assist the reader to respond to a suspicion or reported allegation of fraud or financial irregularity in the most appropriate manner.

Part 2 of the document outlines exactly how a suspicion of fraud or financial irregularity is to be investigated and is only applicable to managers.

Fraud is taken to mean all those activities involving dishonesty and deception that can drain value from MFRS, directly or indirectly and regardless of whether or not there is personal benefit to the fraudster. Included within this definition is:

- Theft, eg of cash, computers, etc
- Deliberate misstatement in the accounting records,
- Bribery and corruption, and
- Non-arms length transactions (eg selling off a piece of land for less than its true worth)
- Indeed it is possible that an allegation in itself can be fraudulent and result in a drain in resources if it is mischievous or vexatious and requires unnecessary investigation.

MFRS is committed to the highest ethical standards and requires all employees to be aware of and comply with their respective Codes of Conduct. All employees of MFRS should act with integrity at all times and should not engage in fraudulent activity of any kind.

Part 1 – For all Staff

Who to inform:

1. If you believe you have good reason to suspect an employee of fraud or any financial irregularity involving MFRS you should discuss it in the first place with your line manager. If a manager believes the incident requires further investigation they must inform the Executive Director of Resources (as Chief Financial Officer) or the Executive Director Legal and Human Resources (statutory Monitoring Officer)
2. However, if you suspect your manager of involvement in the fraud or the issue is particularly sensitive you should speak directly to the Executive Director of Resources or the Executive Director Legal and Human Resources. They will decide on the next course of action which, if the suspicion seems well founded, will involve contacting an appropriate person such as a Locality Manager, or Internal Audit.
3. If you feel unable to speak to the appropriate manager, you can use the MFRS Confidential Reporting Policy and contact the Executive Director of Resources or the Executive Director Legal and Human Resources or Internal Audit. You may obtain advice guidance on how to pursue matters of concern from D.Wright, Executive Director Legal and Human Resources, Service Headquarters, Bridle Road, Liverpool L30 4YD, tel. no. 296 4108

Your suspicions will be logged but in a form that does not undermine your confidentiality.

4. If you are unwilling to raise your concern within MFRS, then you could contact the charity Public Concern At Work (telephone 020 7404 6609 or email helpline@pcaw.co.uk). They will provide confidential advice, free of charge, to anyone concerned about wrongdoing at work but who are not sure whether or how to raise the concern. If you do take the matter outside of MFRS, you should ensure that you do not disclose confidential information or information which is legally protected.

What NOT To Do:

- Information about the fraud or financial irregularity must not be disclosed to the press, committee members, or made public without the authority of the Chief Fire Officer. In accordance with the Code of Conduct, all contact with the press must be made via the Director of Communications unless you are specifically authorised to make contact yourself by the Chief Fire Officer.

- In order to preserve the evidential trail you should not tamper with the suspect's pc, mobile phone or any other electronic device which they own or use.

- You should not make the suspect aware of your suspicions or share your suspicions with anyone other than those with the proper authority.

Points To Consider:

In deciding whether or not to refer a suspicion to a manager you should consider the following points:

- what information do you have and what is the quality of that information?
- what are the credibility and motives of the whistleblower ?.
- Is supporting documentation available or is the allegation / suspicion based on hearsay evidence ?
- Has more than one person corroborated the allegation ?
- Is there any history of a bad relationship between the whistleblower and the accused ?
- Would the whistleblower gain in any way by action being taken against the accused ?
- Is it likely that all the relevant details of the allegations and that all allegations have been made known to you ?
- How serious are the implications of what you know currently if it were true ?
- Do you understand the potential risks if the choice were made not to fully investigate the allegations ?

Merseyside Fire and Rescue Authority has at times received significant numbers of malicious and mischievous allegations of fraud and in considering any allegation you should bear that in mind.

**Merseyside Fire and Rescue Service
Fraud Response Plan**

All allegations must be evaluated objectively. You must consider the facts as they appear, based on the information you have been given. If you are in any doubt then report your suspicions anyway.

Part 2 – For Managers

1 Initial Action To Take Upon Receipt of Reported Suspicions of a Fraud or Irregularity

Step	Action	When	Responsibility
1	<p>Log</p> <p>Brief details of the suspicion raised should be recorded.</p> <p>This log will contain details of all reported suspicions, including those dismissed as minor or not investigated. The log WILL NOT record the names of those staff making the allegations who wish to remain anonymous</p> <p>Person logging the suspicion must also inform their line manager.</p> <p>If the allegation is made anonymously by phone then you should ask the caller to call back in the next 1 to 2 weeks in order that any further information obtained by then can be verified back.</p>	Within 24 hours of receiving the allegation / suspicion	Person who first received details of the suspicion
2	<p>Notification of All / High Value and Sensitive Cases</p> <p>The Manager should confidentially brief the Executive Director of Resources and appropriate Committee Member of all high value and / or sensitive allegations (including those involving senior Officers and or those which could potentially involve the police).</p> <p>Other Officers (including Executive Director of Law and Human Resources), Committee Members and Audit Commission should be informed on a need to know basis by the Executive Director of Resources</p>	When decision is made to investigate the allegation / suspicion, as well as during the course of the investigation	Manager
3	<p>Investigation Team</p> <p>The person assigned to lead the investigation should consider the extent and type of investigation that will be conducted and hence the skills and experience required of the staff to be assigned to the case.</p> <p>Consideration should be given to involving Internal Audit or seeking their advice.</p>	When decision is made to investigate the allegation / suspicion.	Lead Investigator

How to evaluate suspicions:

You initially need to assess what information you have, the quality of that information and, if relevant, the credibility and motives of the whistleblower. In particular, you should ask yourself the following questions:

- Is supporting documentation available or is the allegation / suspicion based on hearsay evidence ? (Merseyside **Fire and Rescue Authority has at times received significant numbers of malicious and mischievous allegations of fraud and in considering any allegation you should bear that in mind**)
- Has more than one person corroborated the allegation ?
- Is there any history of a bad relationship between the whistleblower and the accused ?
- Would the whistleblower gain in any way by action being taken against the accused ?
- Is it likely that all the relevant details of the allegations and that all allegations have been made known to you ?
- How serious are the implications of what you know currently if it were true ?
- Do you understand the potential risks if the choice were made not to fully investigate the allegations ?

Urgent steps:

If the decision is made to investigate the allegation / suspicion, you then need to plan for a successful investigation and consider what **urgent** steps may need to be taken to:

- ❖ Preserve key evidence to maximise future recoveries and / or the chances of a successful investigation;
- ❖ Mitigate further loss;
- ❖ Check for other fraud problems;

Depending on the evidence and information at this time, these steps may include the following:

- changing a financial procedure;
- suspending payments;
- moving staff to another post or suspending them; and/or
- safeguarding files and any other potential evidence.

Such steps should be taken as promptly as justified by the circumstances, but not before consulting with the Director of People & Organisational Development and Director of Finance.

Taking the correct steps within the first 48-72 hours can often be crucial to the direction / success of an investigation.

2 Planning for Success

If, after serious evaluation of any allegations made or suspicions raised, it is decided that further investigation is required, the Lead Investigator needs to consider the following:

<p>1) what are your objectives ?</p>	<ul style="list-style-type: none"> • Take appropriate disciplinary action against relevant individuals (see appendix A for definitions of various acts); • initiate criminal action against relevant individuals; • Take civil action for recovery of funds / assets; • Identify weaknesses and hence recommendations for improvement in MFRS controls and control environment; • Report to professional bodies • Report to relevant regulators and Audit Commission; • Minimize internal and external publicity.
<p>2) how will you run the investigation ?</p>	<ul style="list-style-type: none"> • Who should be made aware of the investigation ? Is it a Police matter – should they be informed now or later • Reporting lines within the investigation team and MFRS as a whole • Do you need external expertise • Do you need Legal / HR expertise to advise on employment issues; • Co-ordination of resources and knowledge within investigating team (e.g. HR, External Specialists and Senior Management); • Consider any previous (audit commission or internal audit) reports in the area under investigation
<p>3) how can you reduce the risks ?</p>	<ul style="list-style-type: none"> • Understand the rights of the subject (so that charges of constructive or unfair dismissal are avoided). • Consider suspension and withdrawal of formal authorities / powers of subjects • Withdrawal of other informal authority and the need to keep trusted Senior Officers and Committee Members informed; • Protect partnership / customer / supplier contacts; • Protect MFRS reputation; <p>Note: Any decision concerning suspension and withdrawal of authorities must be made by an officer at the level of Area Manager or equivalent , NOT the Lead Investigator.</p>
<p>4) how can you maximise potential recoveries</p>	<ul style="list-style-type: none"> • Protect evidence, including hard documents, electronic documents and data, and knowledge of individuals’; • If a high value case then consider freezing subject’s assets.

Criminal v disciplinary proceedings

The decision to initiate criminal proceedings entails the application of different criteria and standards of proof than that applicable to internal disciplinary action, and is dependent on the quality of evidence and proof available. A decision to refer matters to the Police with a view to initiating criminal proceedings is the joint responsibility of the Executive Director for Resources and the Executive Director for Law and Human Resources.

Where criminal proceedings are underway, then consideration should be given as to whether or not to suspend the disciplinary action pending the conclusion of criminal proceedings. However, where disciplinary and criminal proceedings are both justified, they can be pursued concurrently and this may be particularly appropriate where a criminal investigation seems likely to be lengthy and/or indecisive. If concurrent action is taken, care should be taken not to hamper any wider police action (e.g. by alerting other parties).

MFRS will usually agree to police requests to provide information or assistance in support of their criminal investigations. But disclosure, its nature and extent, will depend on the facts of the case. The Executive Director for Law and Human Resources must be consulted before any request for the release of documents or information is complied with. Requests for disclosure of information from other bodies e.g. banks, should be treated in the same manner

A brief summary of the main differences between civil disciplinary and criminal proceedings is set out in appendix B

3. Extent of Fraud

- Before starting to capture relevant evidence you should evaluate the implication of the alleged fraud / irregularity. Fully explore other opportunities for fraud by the suspect. Dishonesty may not be restricted to only one area of the subject's work.
- Consider the possibility of similar frauds having happened in other fire stations, offices, etc.
- Consider the possibility of collusion between staff and with third parties. Is the fraud an indicator of entrenched fraud?
- Re-consider what urgent steps may be required (see section 1 above)

4. Secrecy, Discretion and Managing Publicity

- Consider who needs to know about the investigation? Only those already informed at the outset? Should more Senior Managers or Committee Members be informed as the investigation proceeds? Does the Audit Commission or Internal Audit need to be briefed on findings to date?
- Consider any Freedom of Information exemptions when setting the scope of the investigation
- What is the most effective way to respond to the Press? Consider agreeing on a press notice with the personnel department and the communications department
- Have all staff been told how to deal with telephone calls or questions posed at the reception area? What are the implications of press interest on the investigation and on the reputation to MFRS?

5. Capture and Control of Evidence

During this phase of the investigation you may need to make decisions on the following:

- ✓ Do you know where relevant evidence may be held within MFRS ? Headquarters, fire station, etc. What consents may be needed to access / seize it in a controlled manner ?
- ✓ What relevant legislation and guidance (eg Data Protection Act, Information Commissioners Codes) must you consider when accessing and using such evidence ?
- ✓ What are the potential consequences for the investigation if information is lost or is deemed to have been tampered with – can it be obtained from other sources (eg headquarters) ?
- ✓ What level and quality of evidence is required (e.g. for criminal action to be taken, the integrity of evidence needs to be “beyond reasonable doubt”) ?
- ✓ What is the cost/ benefit of gathering more complete information ?
- ✓ How can you best ensure that the audit trail of information / documents obtained is maintained in a controlled manner ?
- ✓ Should information be sought from suppliers, members of the public or ex-employees (given the effect on reputation and on-going relationships) ?
- ✓ Do you have the skills to download and review information from the IT systems in such a manner that the integrity of the data will be maintained [eg simply opening an electronic file can render the information contained in it inadmissible as evidence in a civil or criminal case] ? If not, consider contacting Internal Audit if you haven’t already done so.

You must take a systematic approach to the collection and analysis of information. You should secure and catalogue potential evidence, protecting its integrity so that it can later be relied on in the event of disciplinary, criminal or civil action. This will include taking the following action:

- Obtaining and securing relevant original documentation;
- Restricting access to the original documentation to those on the investigation team;
- Logging the secured documentation in the agreed appropriate format;
- Taking working copies of relevant documentation, so that the originals are not damaged or written on;
- Taking expert advice on obtaining electronic information (such as emails and accounting records) and, in particular:

- Having experts image laptops / PC's so that the information, data and audit trail is not corrupted, destroyed or lost;
- Ensure back-up copies of electronic data are maintained and not automatically over-written after a certain period of time
- Processing the electronic information into a readable format.
- It is likely that you will need to analyse documents and information to identify patterns and connections. This may include the use of databases, charts and other IT investigation tools.

6. Interviewing

A whole range of people can provide useful information to the investigation. However, you need to understand the risks involved in speaking to each of these potential sources and determine how best to manage them – often determining the appropriate sequence in which to conduct the interviews can be important as well as trying to discourage interviewees from sharing or discussing the subject matter of the investigation / evidence with others. Key risks attaching to different categories of interviewee include:

Interviewee	Risks
Subject	<ul style="list-style-type: none"> ▪ Potentially untrustworthy; ▪ Once aware of investigation, action could be taken to destroy potential evidence / protect assets / obtain alibis.
Staff	<ul style="list-style-type: none"> ▪ Effect on staff morale; ▪ Loss of confidentiality ▪ Possibly working in collusion with subject.
Ex-Employees	<ul style="list-style-type: none"> ▪ Loss of confidentiality; ▪ Loss of reputation.
Supplier / General Public / Partnership staff	<ul style="list-style-type: none"> ▪ Loss of reputation;
Informant, eg member of the public	<ul style="list-style-type: none"> ▪ Potentially untrustworthy; ▪ Problems with admissibility of evidence.

When conducting interviews you need to be mindful of the following:

- ❖ Individuals' rights under the Human Rights Act and their conditions of service (e.g. right to be accompanied during the interview; appropriate breaks; interview being seen to be fair to the individual and properly conducted without being oppressive);
- ❖ MFRS employment policies (discipline, conduct, grievance) must be adhered to
- ❖ Always have two individuals undertaking interviews;
- ❖ Consider method of recording evidence – tape, handwritten notes;
- ❖ Consider preparing witness statement from notes for interviewee to sign.

7. Reporting

At this stage, you will need to (re-)assess:

- Whether criminal action (which would require reporting to the Police) should be taken;
- What the chances are of civil action and asset tracing being successful;
- Whether there are disciplinary reporting or case issues;
- The best way to handle publicity within and outside of MFRS;
- What changes in controls, personnel and accounting records are required;
- Whether any external bodies are to be informed (eg professional bodies, regulators, Audit Commission)
- How MFRS can learn from the fraud.

The report should cover the following areas:

- 1 The nature of the fraud and how it has occurred;
- 2 The quantum / size / scale of the fraud;
- 3 Person(s) responsible;
- 4 Supporting documentation / evidence
- 5 Likelihood of recovery of assets;
- 6 Recommendations for improvements to controls / systems [possibly as separate report depending on report recipients and nature of the case]
- 7 The extent to which it is thought that the full extent of the "issues" have been established
- 8 Further action recommended (e.g. suspension/ dismissal of individuals; report to other bodies, such as Police, Regulators, Professional bodies).

8. Asset Tracing

You need to consider the viability of recovering assets both at the planning stage of the investigation, during the investigation and once a conclusion has been drawn on the strength of the evidence of a fraud having been committed against MFRS.

Key questions you need to consider are:

- ❖ Will it be possible to define the financial loss MFRS has suffered from the fraud ?
- ❖ What are the chances of recovery ? Will the individual be co-operative or will legal action be required ? Has the individual either got the proceeds of the crime, or does he / she have other assets of value ?
- ❖ What are the likely costs of successful asset tracing against realistic benefits ?
- ❖ Is specialist assistance required to help you trace the assets ?

9. Reflection and Lessons Learnt

What are the implications of the incident?

- Evaluate the factors which enabled the fraud to happen. Has the service got effective high level and detailed fraud risk assessment processes and high level and detailed fraud risk controls etc?
- Are there skills issues surrounding an incident?
- Is there a need to raise awareness of reporting mechanisms; is there poor fraud awareness amongst staff?
- Is fraud risk management an integral part of MFRS risk management process? Does fraud risk need to be given a higher profile both amongst the Corporate Leadership Team and also at firefighter level ?
- Identify if MFRS need the assistance of Internal Audit or the Audit Commission to develop workshops, or provide diagnostic reviews to enable them to deal with these issues.

The Lead Investigator should ensure that Fraud / Irregularity records are updated with the outcome of the investigation and issues uncovered. The record can then be used to identify areas, stations, etc of particular risk of fraud.

Within a week of the investigation ending, the Lead Investigator should hold a debrief with the investigation team to determine:

What lessons can be learnt in terms of how they responded? The drivers behind the incident? What could be done better next time?

Appendix A – Definitions of Gross Misconduct and Various Fraud Related Terms

Gross Misconduct

The following are non-exhaustive examples of gross misconduct, which are set out in employees contracts of employment:

- Unauthorised removal of the authority's property
- Offences of dishonesty
- Sexual offences
- Sexual misconduct at work
- Fighting
- Physical assault
- Falsification of time sheets, clock cards, subsistence and Expenses claims etc.
- Theft
- Malicious damage to Authority property

The list of examples of offences of gross misconduct shown above is neither exclusive nor exhaustive, and there may be other offences of a similar gravity, which would also constitute gross misconduct.

Appendix B – Civil & Criminal Action

	Disciplinary	Civil	Criminal
Burden of proof	Balance of probability	Balance of probability	Beyond reasonable doubt
Cost to MFRS	None, other than time of staff attending meetings and tribunals, etc. If a case is taken to the Employment Tribunal, some legal costs may be incurred	Court fees, legal fees, the costs of which depend on complexity of case	None, other than time of staff attending meetings with police and court
Potential Outcome for MFRS	No financial compensation but appropriate sanctions imposed as punishment, which may include dismissal, depending on the gravity of the matter which would potentially prevent further misconduct by the employee and act as a deterrent to others.	Compensation for losses, damages, interest and costs	No financial compensation but appropriate sanctions imposed as punishment which may result in subject getting criminal record and possible custodial sentence, which would potentially prevent further misconduct by the employee and act as a deterrent to others.