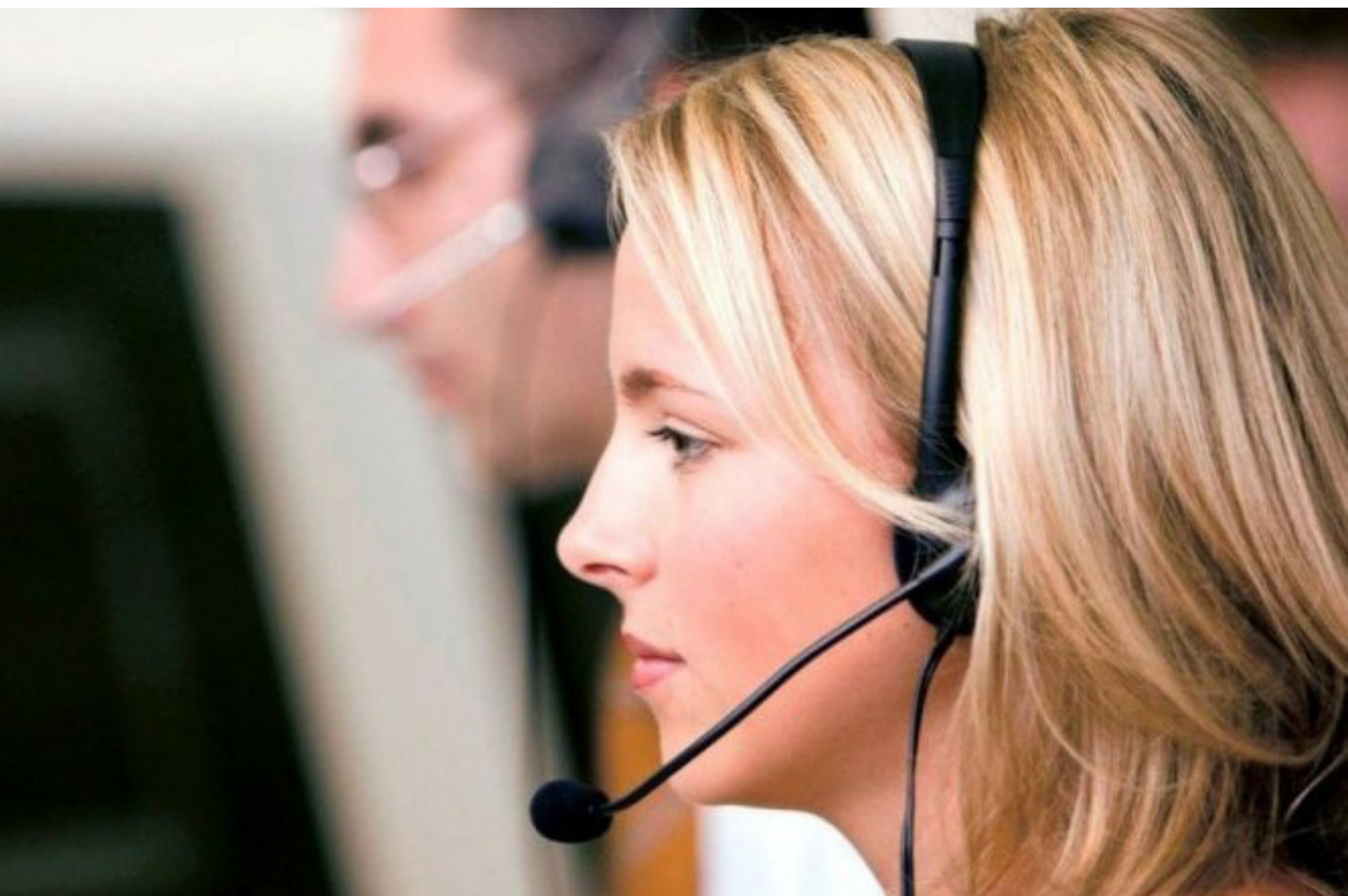




Call centre fraud



Call centre fraud

Good practice guide

This guide is intended for customer call centres regarding employee dishonesty and the prevention of data theft.

Introduction

Call centres are an important and growing business for the economy. Customers' financial details need to be protected from employees who may decide on criminal actions and fraud with such information as is available. It is important to have efficient processes for recruitment, training, internal security and the protection of data to minimise any opportunity for criminal activity.

This information is intended to offer advice to businesses operating customer contact centres, with a view to reducing their exposure to the risk of crime and employee fraud.

Staff recruitment and vetting

All potential employees should be the subject of sufficient checks prior to their employment.

Always undertake a Criminal Records Assessment, for details of how to proceed go to www.crb.gov.uk

Always take up references and where required follow up by making phone calls to referees.

Establish service level agreements with recruitment agencies to ensure that staff employed via this medium are also sufficiently vetted.

Staff security processes

To reduce the risk of any criminal activities call centres should, at a minimum, implement the following practices:

- Contracts of Employment should incorporate the right of management to implement random security searches of staff and belongings;
- Call centre environments should operate a clean room/desk policy;
- Staff should have access to lockers, located away from their work station for personal belongings;
- Internet access, mobile phones, memory sticks and any other devices capable of capturing and removing information should be prohibited for employees when on duty on the call centre floor;
- Staff notepads should be strictly controlled, numbered and security marked to ensure no removal from the pad and the call centre. Ideally desktop whiteboards should be used to allow staff to record temporary details;
- Staff should have a unique and secure access code to allow for the clear auditing of activity whilst working.

Staff training should include

- Awareness of constant monitoring to check for fraudulent activity
- Clear procedures for reporting any suspicions
- Clear do's and do not's for staff

A 'whistleblower' confidential phone line can prove very successful.

Training should incorporate the likelihood prosecution for Fraud or Money Laundering offences including the Proceeds of Crime Act 2002 (possible prison term exceeding 10 years on conviction). The Data Protection Act offences now also carry custodial sentences.

Posters should be clearly displayed to highlight staff roles, protocols and relevant contact numbers.

Good practice and security access

All call centre advisers should only have limited access to the customers' financial details

- New customers providing full particulars should be processed by a 'secure department' where staff have been suitably checked and/or have otherwise proved their reliability;
- Full passwords should never be available to staff – only certain, random characters;
- Bank account information should be restricted unless necessary for the business process;
- Customers should be advised at the beginning of each call that they will only be asked to provide limited characters from their password and not the full code/word or personal information;
- Security questions should be varied rather than standard questions such as 'mother's maiden name'; All call centre advisers should only have limited access to the customers' financial details.
- Consideration should be given to two levels of information for account access rather than just the one password e.g. two digits from the password and an answer to a security question (one of five questions that can randomly appear).

People who are determined to commit crime will continually probe systems and procedures for 'soft spots' that can be exploited. Constant vigilance and a continuous updating of security procedures is essential.

In terms of stolen data it is unlikely that the call centre employee will be the end user of the information. Therefore supervisors and security staff should note any changes to patterns of behaviour or anything of a suspicious nature that might indicate data is being stolen/copied.

Whistleblowing

Whistleblowing has proved to be a very effective deterrent to many forms of employee criminal or dangerous behaviour. Management needs to create a culture in which reporting wrongdoing is not viewed as 'snitching' but rather as protecting the jobs and safety of the rest of the workforce.

This concept can be introduced during the induction of new staff and reinforced during training, by the placement of posters and other reminders that informing about suspicious activity is part of being an 'active citizen'.

Set out below is a list which is intended to illustrate the sorts of issues which may be considered as malpractice or wrongdoing and can be identified as whistleblowing.

- Any unlawful act, whether criminal or a breach of civil law, failure to comply with legal obligations or where a miscarriage of justice has occurred, is occurring or is likely to occur;
- Maladministration, as defined by the employer;
- Breach of any statutory Code of Practice;
- Breach of, or failure to implement or comply with any policy determined by the employer;
- Failure to comply with appropriate professional standards;
- Corruption or fraud including obtaining money without entitlement;
- Misuse of assets, including stores, equipment, vehicles, buildings, computer hardware and software;
- Endangering the health and safety of any individual with actions which are likely to cause physical danger, or to give rise to a risk of significant damage to property.

Anti fraud and corruption

Local authorities and other public bodies should also consider making staff aware of the following measures to tackle fraud and corruption.

- Failure to take reasonable steps to report and rectify any situation which is likely to give rise to a significant avoidable cost, or loss of income, to the employer or would otherwise seriously prejudice the employer;
- Abuse of power, or the use of the employer's powers and authority for any unauthorised or ulterior purpose;
- Unfair discrimination in the employer's employment or services;
- Causing damage to the environment;
- Deliberately concealing information in relation to any of the items on this list.

Contact the Business Crime Reduction Centre
on 0114 275 1283 or visit our website at www.bcrc-uk.org

Business Crime Reduction Centre, working with South Yorkshire Police to reduce crime against business

Business Crime Reduction Centre
4th Floor, Castle Market Buildings, Sheffield S1 2AH
Tel: 0114 275 1283 Email: info@bcrc-uk.org