



## Contact Centre Fraud

### Good Practice Guide

For Customer Contact Centres Regarding Employee Compromise and the Prevention of Data Theft



## Introduction

Customer Contact Centres are an important and growing business for the Scottish economy. Customers' financial details need to be protected from unscrupulous employees who may revert to criminal actions and fraud with such information. It is important therefore to have efficient processes for recruitment, training and internal security of data to minimise any opportunity for criminal activity.

This document is intended to offer advice to all businesses operating Customer Contact Centres, with a view to reducing their exposure to employee or 'insider fraud'.



I.D.

## Staff Recruitment & Vetting

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

Service level agreements with recruitment agencies should ensure that staff, employed via this medium, are also sufficiently vetted.



## Staff Security Processes

**Staff contracts should incorporate the right of management to implement random security searches of staff and belongings.**

**All contact 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 or any other device capable of capturing and removing information should be prohibited for staff when on 'live duties' within the Call Centre floor.
- ◆ Staff notepads, if used, should be strictly controlled, numbered and security marked to ensure no removal from the pad and the call centre.
- ◆ Desktop "whiteboards" should be utilised to allow staff to record temporary details. This negates the need for notepads.
- ◆ All staff should have a unique and secure access code to allow for the clear auditing of activity whilst working.

\*\*42 ..... Customer  
 \*\*672 ..... Customer  
 \*\*3343 ..... Customer  
 \*\*00173 ..... Customer



## Staff Training

Staff Training could include:

- ◆ Awareness of constant monitoring of fraudulent activity.
- ◆ Clear procedures for reporting any suspicions.
- ◆ Clear do's and don'ts for staff.

A `Whistleblower` confidential phone line can prove to be very successful for organisations.

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

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

+44 10 10

+44 10

## Good Practice & Security Access

All contact centre advisors should only have limited access to the customers' financial information.



New customers providing full particulars should be processed by a 'secure department' where staff have been suitably vetted 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 details.



Security questions should be varied rather than standard questions, such as 'mother's maiden name'.



Consideration should be given to 2 levels of information for account access rather than just the one password e.g. 2 digits from the password and an answer to a security question (one of five questions that can randomly appear). It is another layer of security.



## Conclusion

Internal compromise by staff is an existing issue for both the police and business community and this document is intended to inhibit exposure to such crimes occurring. Therefore the integrity of the business and staff are preserved and customer confidence is assured.



## Useful Numbers

Crimestoppers 0800 555 111