



Subject:

Circular Reference: HSS (F) 52/2007

**Fraud Forum Best Practice Guidance
Actions to be taken in the event of a Compromise of
Personal Data: Management Checklist**

30 August 2007

For Action by:

**Chief Executive and Director of Finance of each HSS Board,
HSS Trust, Special Agency and NDPB**

Summary of Contents:

**This circular brings to Accounting Officers' attention DAO
(DFP) 12/07 Fraud Forum Best Practice Guidance - Actions
to be taken in the event of a Compromise of Personal Data:
Management Checklist.**

**The purpose of this circular is to provide advice/guidance on
the actions which you may wish to consider in the event of
personal data being compromised.**

Enquiries:

**Any enquiries about the contents of this Circular should be
addressed to:**

**Sandra Lowe
Counter Fraud Policy Unit
Room D3.9
Castle Buildings
Stormont Estate
BELFAST
BT4 3SQ**

Tel: 028 90 765616

E-mail: Sandra.Lowe@DHSSPSNI.GOV.UK

Related documents:

HSS (F) 76/2006
HSS (F) 73/2006
HSS (F) 69/2006
HSS (F) 44/2006
HSS (F) 62/2005

**Status of Contents:
Action**

**Implementation:
Immediate**

Additional Copies:
Tel: 028 90 523389
www.dhsspsni.gov.uk

**Head of Accountability and
Accountancy Services Division
Ciaran Doran**

Room G2-1
Rathgael House
Balloo Road
BANGOR BT19 7NA
Tel No: 028 9185 8203 (x 68203)
Fax No: 028 9127 7690
email: ciaran.doran@dfpni.gov.uk
and joan.braniff@dfpni.gov.uk



DAO (DFP) 12/07

30 AUGUST 2007

DEAR ACCOUNTING OFFICER

FRAUD FORUM BEST PRACTICE GUIDANCE

ACTIONS TO BE TAKEN IN THE EVENT OF A COMPROMISE OF PERSONAL DATA : MANAGEMENT CHECKLIST

Purpose

1. The purpose of this letter is to provide advice / guidance to Departments, Agencies, NDPBs and other sponsor bodies on the actions which you may wish to consider in the event of personal data being released incorrectly (i.e. being compromised).

Compromise of Personal Data

2. Due to the diverse nature of business undertaken, organisations are required to hold and process large amounts of information relating to individuals (i.e. personal data). While the NICS is committed to ensuring that it complies fully with the principles of the Data Protection Act and in particular the seventh principle which states that 'Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data' there is always the possibility that personal data may become compromised. This could occur by accident, error or by deliberate action.

Identity theft


3. In addition to the embarrassment and negative publicity that this may attract, there is also the potential risk that the information could fall into the wrong hands and that it could assist in the perpetration of identity fraud. Identity fraud is where individuals or organisations find out personal details and use them to open bank accounts and / or obtain credit cards, loans, state benefits and documents such as passports and driving licenses in another's name with a criminal intent.

4. While the compromise of data does not necessarily mean that identity theft will occur, in order to reduce the potential, it is important that action is taken promptly. Annex A seeks to provide Departments with a checklist of actions which they should take account of should such a situation arise.
5. It should be noted that this is not a definitive or exhaustive list of actions which Departments may wish to consider, and that actions taken may need to be tailored to take account of the nature and specific circumstances of the compromise which has occurred.
6. It is also emphasised that this guidance is not intended to detract from, or replace in anyway, the focus and effort which Departments currently place on ensuring that data relating to individuals is adequately protected and safeguarded in line with the Data Protection Act principles.

Action

7. I would ask you to circulate this letter to management in all your business areas and to your sponsored bodies, and in particular to nominated Data Controllers and business areas where there is a responsibility for holding and processing personal data.
8. This DAO has been endorsed by the members of the NICS Fraud Forum and Central Personnel Group. DFP recommend that DAOs relating to Fraud and endorsed by the Fraud Forum, should be formally considered by the Audit Committee.
9. Any enquiries about this letter should be addresses to Alison Caldwell, Fraud and Internal Audit Policy, Tel 02891277633 (network 69033), E-mail: alison.caldwell@dfpni.gov.uk

Yours sincerely



CIARAN DORAN
Deputy Treasury Officer of Accounts

ACTION TO BE CONSIDERED IN THE EVENT OF THE COMPROMISE OF PERSONAL DATA

Actions / Considerations

- Establish the exact nature of the data released, the amount / volume, and the timescale over which the release has occurred and if possible the recipient(s) of the data.
- Ensure immediate action is taken to prevent further compromise.
- If the compromise has been due to personal data being sent to the wrong individual(s), the first indication that that this has occurred may be through contact from recipients. It is important that staff receiving calls / enquiries from members of the public etc. are aware of the details they need to collect and record from callers and the advice / information which should be given out.
- Staff should be aware of the need to alert the nominated Data Controller and Data Protection Officer, and liaise with the Controller to ensure that the Information Commissioner is advised.
- Consider the need to liaise with the police and other statutory bodies taking into account the circumstances of the compromise and the data involved. If required further advice / guidance may be available from the PSNI representative on the NICS Fraud Forum who can be contacted through Fraud and Internal Audit Policy Branch, AASD.
- Alert your Press Office in order that the incident can be appropriately handled in the media.
- The Accounting Officer, Board and Minister as appropriate should be advised and submissions / briefings prepared as required. The need for urgency in addressing the issue should be recognised.

- If appropriate, liaise with the British Banking Association, APACS - the UK payments association, Irish Banking Federation, Irish Payment Services Organisation and the Northern Ireland Bankers' Association. Contact details for each are included at Annex B. These bodies will be able to advise you of the actions required and can be used to alert their members to the incident and to highlight the potential risk. Further, more detailed information of the data which has been compromised should be provided to these bodies as soon as practicable.
- Formally notify those individuals whose personal data has been compromised. Notification should be apologetic in tone and include:-
 - details of the information released;
 - an explanation as to how the compromise occurred if appropriate;
 - the actions that have been taken by the Department (including notification to third parties e.g. Information Commissioner, BBA, APACS, IBF, IPSO, NIBA etc);
 - advice on the actions which can be taken by individuals to protect themselves against the risk of identity theft;
 - contact details for those requiring / seeking further information.

(It may also be useful to refer individuals to the relevant information leaflets and / or advice as contained on the Home Office web site <http://www.identity-theft.org.uk>. These contain useful sources of information for individuals on preventing identity theft.)

- Where it is known that information has been issued incorrectly to others, recipients of the information should also be provided with instructions on what to do with the information they have received. In some instances it may be appropriate and more practical to use the same correspondence to cover both recipients of the data and those whose data has been compromised.
- Consideration should also be given to notifying other interested parties of the general circumstances of the data compromise. This could include for example delivery partners, MLAs / political parties, appropriate voluntary and community

groups, interest groups, trade unions etc. Care should be taken to ensure that in doing so further breaches of the Data Protection act are not committed.

- An investigation and post incident review should be carried out to determine the cause of the compromise and to evaluate the adequacy and effectiveness of the response taken. Where required, control improvements should be implemented and reviews carried out periodically to ensure that controls / systems are operating effectively.
- Depending on the nature and scale of the data compromise it may be useful to establish a Compromise Management Group / Team to coordinate the response to the incident. Representatives may include management from the operational area involved, Customer Services, Personnel, IT, Press Office, and Finance Departments etc. This Group may wish to further consider the need to establish specific team(s) to deal with individuals' queries and complaints. Factors such as accommodation, telecommunications, IT and training for staff handling enquiries should be considered. The establishment of a free phone number for concerned callers may also be useful.

CONTACT DETAILS**Annex B**

<p>British Banking Association (BBA)</p> <p>Richard Cook Director Financial Crime British Bankers' Association Pinnars Hall 105-108 Old Broad Street London EC2N 1EX</p> <p>Tel: 020 7216 8823 / 8800 Fax: 020 7216 8811</p>	<p>APACS – UK Payments Association</p> <p>Jeff Collins Manager, Fraud Intelligence Bureau Fraud Control Unit APACS - the UK payments association Mercury House, Triton Court 14 Finsbury Square London EC2A 1LQ</p> <p>Tel: 020 7711 6355 Fax: 020 7628 5169</p>
<p>Irish Banking Federation (IBF)</p> <p>Robert Rafter Operations Executive Irish Banking Federation 5th Floor, Nassau House Nassau Street Dublin 2</p> <p>Tel: 0353 1671 5311 Fax: 0353 1679 6680</p>	<p>Irish Payment Services Organisation (IPSO)</p> <p>Úna Dillon Head of Card Services & Communications IPSO Ltd 12/13 Cumberland Street Dun Laoghaire Co. Dublin</p> <p>Tel: 0353 1663 6746</p>
<p>Northern Ireland Bankers' Association (NIBA)</p> <p>Bill McAlister Secretary Stokes House 17/25 College Square East Belfast BT1 6DE</p> <p>Tel: 028 9032 7551 Fax: 028 9033 1449</p>	<p>Information Commissioner</p> <p>Information Commissioner's Office - Northern Ireland Room 101 Regus House 33 Clarendon Dock Laganside Belfast BT1 3BG</p> <p>Tel: 028 9051 1270 Fax: 028 9051 1584</p>
<p>Central Freedom of Information Team</p> <p>Dr David Lammey Head of Central Freedom of Information Team Office of the First Minister and Deputy First Minister Room A 5.5, 5th Floor Castle Buildings Stormont Belfast BT4 3SR Tel: 028 9052 8242</p>	