

# **Break in at Royston House – Frequently asked questions**

## **1. What has happened?**

At some stage over the weekend of 30-31 May there was a break-in to Corporate HR premises in Royston House in Belfast city centre. Twelve laptop computers were stolen. Initial investigations indicated that two of these contained a wide range of personal data. All of the laptops were password-protected.

## **2. Was Royston House a specific target?**

No. A number of other adjacent buildings were also burgled.

## **3. What actions are you taking to address this situation?**

There is currently a live police investigation ongoing and an internal security review was carried out by the OFMDFM Security Advisory Unit. We are taking this incident very seriously and a team was set up to deal with the consequences of the break in. To date it has assessed the nature of the information that was contained on the twelve laptops, contacted banks where appropriate and continues to liaise with the PSNI. The Department also took advice from the British Banking Association and submitted a report to the Information Commissioner's office. We are also in contact with the Trade Unions.

## **4. Is data about me involved in this incident?**

Investigations indicated that the data relates in the main to all current and some former civil servants.

## **5a. What details of mine are affected?**

Whilst the initial PSNI view remains that the target of the theft was the hardware other than the data and whilst all the laptops were password protected, there remains a risk to the security of this information and therefore we moved as quickly as possible to contact all staff affected.

One of the laptops contained data that included employee names, home addresses, payroll numbers, national insurance numbers and dates of birth for all civil service employees.

A different laptop contained separate information, namely the bank account numbers and sort codes for a number of staff.

The following lists the key data items:

- Employee Name
- Employee Address or Contact Details
- Email Address
- Employment History
- Employment Position and Grade
- Absence Data
- National Insurance Number
- Date of Birth
- Gender
- Payroll Number
- Organisation
- Equal Opportunity Details
- Staff report history
- Outcome of Occupational Health Service Referrals
- Welfare Rating
- Qualification Details
- Disability Details
- Pension Scheme Type
- Name and Address of nominated primary contact
- Remuneration for March, April and May 2009

## **5b. I am an industrial member of staff – what details of mine are affected?**


Whilst the initial PSNI view remains that the target of the theft was the hardware other than the data and whilst all the laptops were password protected, there remains a risk to the security of this information and therefore we moved as quickly as possible to contact all staff affected.

One of the laptops contained data that included employee names, home addresses, payroll numbers, national insurance numbers and dates of birth for all civil service employees.

A different laptop contained separate information, namely the bank account numbers and sort codes for a number of staff. The following lists the key data items:

- Employee Name
- Employee Address or Contact Details
- Email Address
- Employment History
- Employment Position and Grade
- Absence Data
- National Insurance Number
- Date of Birth
- Gender
- Payroll Number
- Organisation
- Equal Opportunity Details
- Staff report history
- Outcome of Occupational Health Service Referrals
- Welfare Rating
- Qualification Details
- Disability Details
- Pension Scheme Type
- Name and Address of nominated primary contact


## **6. What is identity fraud?**

Your identity and personal information are valuable. Your personal details could be used to open bank accounts and get credit cards, loans, state benefits and documents such as passports and driving licenses in your name. For further details see [www.identitytheft.org.uk](http://www.identitytheft.org.uk) .

## **7. What can I do to ensure that the data is not used fraudulently?**

You should remain watchful:

- if you receive bills, invoices or receipts or see entries in your statements for goods or services which you have not ordered you should contact your bank or building society immediately;
- be aware of anybody who contacts you unexpectedly by phone or email and asks for personal information or account details, whatever company or organisation they claim to represent. If you are at all suspicious contact your bank or building society;
- if your password uses any of your personal data, for example your name or date of birth, you should change any passwords you use.

There is no need to contact your bank as a matter of routine. You can get further information from [www.identitytheft.org.uk](http://www.identitytheft.org.uk) .

## **8. Should I consider changing my bank account to prevent fraud?**

The general advice from the UK Payments Administration (formerly APACS) is not to change bank or building society accounts unless you have evidence that your account has been used fraudulently. The UK Payments Administration is the UK trade association for payments and for those institutions that deliver payment services to customers.

As always, you should be vigilant and follow existing security advice to help you spot and stop ID fraud being committed using your details. This includes always checking your statements, opening post and checking bills, and if you spot an unfamiliar transaction you should contact your bank, building society or service provider immediately.

## **9. Will I be reimbursed for any losses that I incur as a result of this incident?**

If you are the innocent victim of banking fraud, as a UK customer, you are protected by the Banking Code, banking law and practice which means you should not suffer any financial loss as a consequence.

## **10. Can I change my National Insurance Number to protect me from fraud?**

No, it is not possible to change your National Insurance Number. Both HM Revenue and Customs and the Department of Work and Pensions advice is that the National Insurance number is not an ID number. While it is used as a convenient reference by many Government organisations it will not, in itself, provide access to financial accounts or information in either the public or private sector.

## **11. Where can I go for more advice?**

We will continue to update these FAQs. You may wish to refer back.

## **12. Should I change my passwords?**

We would advise anyone affected that if they use any personal data, such as their name or date of birth, they may wish to consider changing their passwords.

## **13. Do I need to contact my bank or building society?**

No, not unless you spot a transaction on your bank account that you didn't authorise.

## **14. If I notice something unusual – if an account has been opened with a bank or business with whom I have no relationship - do I contact them or do I contact the police?**

Contact your bank or financial institution concerned and keep a record of all communication. Dependent on their advice, you should report the matter to your local police station.

If applications for credit have been made in your name you can ask to have any incorrect information removed. The following organisations may be able to help.

- Experian: 0870 241 6212 ([www.experian.co.uk](http://www.experian.co.uk))
- Equifax: 08705 143700 ([www.equifax.co.uk](http://www.equifax.co.uk))
- Call Credit: 0870 060 1414 ([www.callcreditcheck.com](http://www.callcreditcheck.com))

## **15. How is my personal security being addressed?**

PSNI remain of the view that the target of the theft was the hardware rather than the data. There is no evidence to suggest that any of the data contained on the stolen laptops has been compromised or that it has fallen into the wrong hands. Should this situation change, we will contact you again.

PSNI have conducted an overall assessment of the threat to those individuals whose details were contained on the stolen items. The PSNI threat assessment letter says that there is nothing to suggest that the theft was carried out by individuals linked to Irish Republican Terrorism. PSNI have also advised that there is no information to indicate that personal details have fallen, or are likely to fall, into the hands of Dissident Republicans, although the possibility cannot be ruled out. This situation is monitored by PSNI, and the OFMDFM Security Advisory Unit will be advised of any change.

## **16. Who is managing the incident?**

The PSNI investigation is on-going. The Director of Personnel in the NICS, Derek Baker, was in charge of the overall management of the NICS response to the incident in its immediate aftermath. An incident team was set up and managed all aspects of the incident, including communications with staff, analysis of the information contained on the stolen laptops, engagement with PSNI, the banks and others involved as appropriate, and the provision of reports to the Information Commissioner. The incident team has now been stood down, though DFP continues to liaise with the PSNI and respond to queries about the incident as appropriate.

## **17. Why was my personal data on a laptop?**

All the circumstances of this incident have been the subject of a full independent investigation, from the physical security of the building through to the management of information. The data was held as part of a major data migration exercise from the

legacy Human Resource Management System to the new HR Connect personnel service. Data relating to remuneration was also held for financial management purposes. A copy of the Cabinet Office Review is available at the following link - [http://www.dfpni.gov.uk/cabinet\\_office\\_royston\\_review\\_report.pdf](http://www.dfpni.gov.uk/cabinet_office_royston_review_report.pdf)

## **18. Were the stolen laptops and/or passwords encrypted?**

No.

## **19. Where do I stand legally on gross negligence of loss of personal data?**

Staff may have felt upset or inconvenienced by the theft of the laptops. These are normal human emotions and no compensation is available in law for that.

There is no evidence that any data on the stolen laptops has been accessed or used and therefore no evidence that any loss has been caused. Steps had been taken to protect the laptops and data and it needs to be recognised that this incident was the result of criminal action that is currently the subject of a PSNI investigation. Therefore the department does not accept liability for loss or cost that staff may incur.

## **20. Why does DFP have my personal information when I work/worked in a different department?**

Over the last 25 years DFP has carried out a centralised management system for personnel data for staff across all NICS Departments.

## **21. Why has everyone not received the same email?**

All staff were sent an initial email on 1st June advising them of the break-in to Royston House; a more detailed email was sent to all staff on 3rd June; in addition to this some individuals were contacted separately and immediately, on 3rd June, as these individuals' banks or building society account details were contained on one of the laptops. Their banks were also notified immediately. It took longer to identify

others due to the arduous and time consuming task of examining the data in detail. The incident team was established immediately following the theft and an examination of the data commenced. It took some time but when individuals were identified, notifications were issued as soon as was practicable

## **22. Is the information on the stolen laptops easily retrievable?**

All of the laptops stolen were protected by passwords but we are working on the basis that the information stolen is vulnerable and we have taken action to mitigate the risk of fraudulent use of any of the personal data held on the laptops. The information is held in a variety of formats and potentially could be retrieved.

## **23. How many staff are involved that had bank details revealed?**

The Bank details of around 900 staff were held on one of the stolen laptops.

## **24. How were the laptops stored in Royston House and was it in accordance with security guidelines?**

The stolen laptop computers were stored in Royston House in accordance with current policy.

## **25. How secure was my information when it was carried around from place to place?**

It should be remembered that the laptops were stolen from the workplace, where they were stored in accordance with current policy. The information was held on password protected laptops. The information was not breached at any stage prior to the break-in and there is no evidence to date to suggest that it has been breached following the break-in.