www.pdpjournal.com

ISSN 1473-3498

Privacy & Data Protection

Volume 8, Issue 2

December 2007

25 million affected by 'deeply disturbing' HMRC data breach

A UK government department has caused the largest data loss in the UK's data protection history. Chancellor of the Exchequer, Alistair Darling, revealed that Her Majesty's Customs and Revenue ('HMRC') lost two CDs containing personal details of 25million child benefit claimants.

The missing discs, which detail the identities and finances of 7.25 million British households, include information such as names, addresses, birth dates, national insurance numbers and bank account details of every child benefit claimant in the country.

The unencrypted CDs were sent in the post at the end of October by a junior employee at the HMRC office in Tyne & Wear. The CDs were intended for the National Audit Office ('NAO'), but were lost in transit and have not been seen since. A second set of CDs were then sent by recorded delivery, even though procedure requires the discs to be carried by an escorted driver or wired electronically to the National Audit Office.

The Chancellor and the Prime Minister, Gordon Brown, have known about the loss since November 10th, yet the police were not told for a further five days—the banking industry and the public were the last to be alerted to the data breach. Officials at HMRC believe the discs have not fallen into criminal hands, but urged people to monitor bank accounts "for unusual activity."

As a consequence of the breach, the Chairman of the HMRC, Paul Gray, has resigned. Mr Darling apologised for what he described as an "extremely serious failure on the part of HMRC to protect sensitive personal data entrusted to it in breach of its own guidelines." Richard Thomas, Information Commissioner, said "this is a deeply deeply disturbing saga. It brings home the-

(Continued on page 17)

Online black market for bank details

Financial details of thousands of Britons are being sold for as little as £1 on more than 100 trafficking websites, it has been revealed.

The private account numbers, PIN numbers and security codes were offered as tasters by illegal hacking sites in the hope that purchases would follow. A *Times* journalist successfully downloaded banking information of 32 people, including a High Court deputy judge and a managing director, for free.

A spokesman for the Information Commissioner's Office said, "we will be looking at the evidence provided and we are investigating the circumstances. This looks serious and is a matter of genuine concern."

The spokesman added, "we can take action against UK-based organisations that flout the Data Protection Act. If some of these websites are not UK-based we will work with our counterparts in the relevant country."

He said the investigation would initially focus on what security breach, if any, had taken place to allow the information to get into the public domain in the UK. Preventing unlawful disclosures or losses by organisations is a priority.

If the data was acquired fraudulently, or by theft, the matter would be passed to the police as a criminal inquiry.

Headlines:

- FCO undertaking after visa website security failures, p.17
- New ICO warning about social network risks, p.18
- Doctors may be fined for losing laptops, p.19
- ID scheme on rocks? P.20

Inside this issue: