R K

The Facts

Between 18 May 2015 and 30 July 2015 a "Network Attached Storage" device (the "Device") was taken offline and stolen by a member of staff, or a contractor, from a data server room at Royal & Sun Alliance Insurance PLC ("RSA"). An access card and key were required to enter the data room and 40 people were permitted access to the data room, some of whom were non-essential.

The Device contained personal data including 59,592 people's names, addresses, bank account and sort code numbers and 20,000 customer names, addresses and credit card 'Primary Account Numbers'. However, no expiry dates or CVV numbers were on the Device. The Device was also password protected, although it was not encrypted. The Device has not been recovered.

The Law

The Information Commissioner's Office (the "ICO") considered whether the abovementioned facts amounted to a breach of the Data Protection Act 1998 (the "DPA").

The ICO held that as RSA are a data controller for the purposes of the DPA, they have a duty to comply with the data protection principles with regards to all personal data of which they are the controller.

The seventh data protection principle states as follows:

"*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*."

In order for RSA to be in breach of the seventh data protection principle the ICO had to find that there was a serious contravention of the DPA, of a kind which was likely to cause substantial damage or distress. The ICO also had to find that the contravention was either deliberate, or RSA knew or ought to have known that there was a risk that the contravention would occur and would be of the kind likely to cause substantial damage, and that RSA had failed to take reasonable steps to prevent the contravention.

The Decision

The ICO found that RSA had failed to take appropriate organisational and technical measures to protect against the unlawful processing of personal data.

The ICO pointed to the following factors which indicated that inadequate steps had been taken by RSA, namely:

1. they failed to encrypt the datasets prior to uploading them onto the Device;

2. they had failed to physically secure the Device to the data room;

3. they had failed to routinely monitor whether the Device was online, and if it was not raise the alarm;

4. CCTV was not installed inside the data room;

5. they had failed to restrict access to the data room to only essential staff and contractors;

6. they allowed staff and contractors to enter the data room unaccompanied; and

7. they failed to monitor access to the data room.

Further, the ICO held that due to the nature of the personal data held on the Device, the potential consequences of the Device being taken were substantial and the consequences were likely to cause significant distress to the customers if the information was misused.

The ICO suggested possible steps which RSA could have taken in order to ensure that they did not fall foul of the seventh data protection principle. These included, using encryption; physically securing the device in the data room; routinely monitoring the Device and whether it was online; installing CCTV in the data room; restricting access to the data room to essential staff; and/or auditing access logs to the data room.

The ICO held that in addition to the above, there were certain aggravating factors, specifically the fact that RSA could not pinpoint exactly when the Device was stolen, and that they had received 195 complaints about the incident.

In light of the above, the ICO decided to issue a Monetary Penalty Notice in the sum of £150,000.

Commentary

This case highlights the fact that portable devices are at high risk of loss or theft and, as such, additional security measures need to be taken to protect personal data contained on them. This should help to ensure that the seventh data protection principle is complied with.

The ICO indicated in their decision that where an event is a one-off, or attributable to mere human error the contravention may be considered less serious in terms of company deficiencies. Albeit this was not the case in this instance.

It is an important reminder for all organisations that hold personal data to ensure that they have appropriate measures and controls in place to ensure that the data they hold is adequately protected.

For further information, please contact Georgina Squire or the Partner with whom you usually deal.