# CYBER RISKS & LIABILITIES_
## NEWSLETTER

**February / March 2014**

IN THIS ISSUE



# Guard Your Data When Using Mobile Apps

Apps can do pretty much anything—they can find the best local restaurant, chart the quickest route through snarled city traffic and track weight loss. Unfortunately, they can also steal your data.

The Information Commissioner's Office (ICO), the United Kingdom's independent authority that upholds information rights in the public interest, recently warned consumers to protect their personal information when downloading mobile apps. The warning was meant to temper the unbridled app downloading that occurs on Christmas Day, the busiest day of the year for app downloads. Apple's App Store downloads rose by more than 53 per cent on Christmas Day in 2013.

Whether your employees use their own devices at work or use company-issued devices, chances are they have downloaded at least one mobile app. A December 2013 ICO survey found that 59 per cent of UK adults have downloaded an app, a figure which the ICO estimates will increase. Make sure your employees know how to keep their devices safe and guard their personal information when using mobile apps.

In order for apps to do the convenient, wonderful things they do, they use customers' personal information, such as physical location, contact details and passwords. Unscrupulous data thieves can steal your employees' devices and gain access to this valuable information, or siphon it through a rogue app that your employees downloaded without knowing it was malicious. Hackers do this by adding their own illegitimate elements to a popular app and then offer it for free on a 'bulletin board' or through a fake online store. Once employees download the phony app, hackers may have unfettered access to their devices.

To help thwart data theft attempts, encourage your employees to follow these ICO top tips for securing personal information when using apps:

- Download apps only from official, trusted stores. Be extremely wary of apps from unknown sources.
- Read the information available about an app in the app store before downloading it. Verify that you are comfortable with the amount and type of personal information it will be using.
- Clear out unused apps regularly—inactive apps are an open invitation to thieves. If you no longer use an app, uninstall it.
- Install mobile security software to defend your device.
- Erase any apps from the device before you recycle, resell or donate it, since they may have access to your personal information. Activate the 'factory reset' option in the device's settings.

Crendon Insurance Brokers

# Require Data Protection Training for Temporary Workers

The Information Commissioner's Office (ICO) recently warned employers to ensure their temporary workers receive adequate data protection training. The danger of neglecting to provide sufficient data protection training is illustrated by four data breaches at the Great Ormond Street Hospital for Children NHS Foundation Trust.

The data breaches were caused by sending letters with personal health information to the wrong addresses. They all occurred between 28 January 2012 and 18 June 2013. Three of the four breaches were the result of inadequate data protection training for temporary staff, despite their roles routinely involving handling personal information. The trust was also woefully unprepared for a data breach, with no measures in place to check whether letters were addressed to the correct address before they were sent. After an investigation, the trust was required to sign an undertaking with the ICO that stipulated plans for improving data protection.

If you hire temporary workers who handle personal information, make sure to comply with the eight principles of the Data Protection Act that ensure personal information is:

- Processed fairly and lawfully
- Handled for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Kept only for the necessary amount of time
- Managed in line with individual rights
- Stored only in countries with adequate data protection laws
- Secure

## Pay day loans company fined for millions of spam texts

The ICO served the pay day loans company First Financial with a £175,000 penalty after an investigation revealed that the company was responsible for sending millions of illegal spam texts. Organisations must have an individual's consent before sending marketing messages via text, according to the Privacy and Electronic Communications Regulations, which govern electronic marketing. The penalty comes shortly after First Financial's former sole director was prosecuted for failing to report that his company was processing personal information. The sole director was personally fined £1,180.66.

## Surgery manager illegally accessed medical records

The former finance manager of a GP's practice in Maidstone was prosecuted after he accessed the medical records of approximately 1,940 patients registered with the practice. The manager was fined £996 and ordered to pay a £99 victim surcharge and £250 in prosecution costs. Between 6 August 2009 and 6 October 2010, he accessed patients' records on 2,023 occasions. Most records belonged to women in their twenties and thirties. The manager repeatedly accessed the record of one woman, believed to be his school friend, and her son. His motives remain unknown. Unlawfully accessing personal data is a criminal offence, punishable by up to £5,000 in a Magistrates Court or an unlimited fine in Crown Court.

## Private investigators unlawfully obtain information

Two private investigators were found guilty of conspiring to breach the Data Protection Act by operating a company that conned organisations into revealing personal details about customers. The investigators' job—recovering individuals' past debts on behalf of clients—was legitimate, but their methods were not. Through their company, the investigators routinely tricked organisations such as utility companies, GP surgeries and TV Licensing into releasing customers' personal information, often by claiming to be the very people they were tracing. The ICO's investigation estimated there were nearly 2,000 separate breaches of the Data Protection Act between 1 April 2009 and 12 May 2010.

CYBERRISKS&LIABILITIES_
NEWSLETTER

**Crendon Insurance Brokers Ltd**
11 Greenfield Crescent
Birmingham, West Midlands, B15 3AU
0121 454 5100
www.crendoninsurance.co.uk