News release

10 May 2011

ICO fines former ACS Law boss for lax IT security

Fine could have been £200,000 if firm was still trading

The owner of former solicitors firm ACS Law has been served with a monetary penalty for failing to keep sensitive personal information relating to around 6,000 people secure, the Information Commissioner's Office (ICO) said today.

Andrew Jonathan Crossley – as data controller of the former law firm - has been served with a monetary penalty of £1,000.

Information Commissioner, Christopher Graham, said:

"This case proves that a company's failure to keep information secure can have disastrous consequences. Sensitive personal details relating to thousands of people were made available for download to a worldwide audience and will have caused them embarrassment and considerable distress. The security measures ACS Law had in place were barely fit for purpose in a person's home environment, let alone a business handling such sensitive details.

"As Mr Crossley was a sole trader it falls on the individual to pay the fine. Were it not for the fact that ACS Law has ceased trading so that Mr Crossley now has limited means, a monetary penalty of £200,000 would have been imposed, given the severity of the breach. Penalties are a tool

for achieving compliance with the law and, as set out in our criteria, we take people's circumstances and their ability to pay into account."

Mr Crossley of ACS Law - which has now ceased trading - specialised in pursuing alleged copyright infringement cases on behalf of copyright holders from the music, video games and adult film industries. The firm had written to thousands of individuals who were alleged to have broken copyright law. They were pursued using information obtained from individuals' internet service providers (ISPs).

In September 2010, ACS Law's website was subjected to an online attack which caused it to crash. After the attack a file containing emails between ACS Law staff, and some to and from ISPs or members of the public, appeared on a website which allowed anyone who downloaded the file access to around 6,000 people's sensitive personal information. This included individuals' ISP account details, their names and addresses, their IP addresses and information about the content they were alleged to have illegally copied. Some of the emails also included people's credit card details, as well as references to their sex life, health and financial status.

The ICO's investigation found serious flaws in ACS Law's IT security system. Mr Crossley did not seek professional advice when setting up and developing the IT system which did not include basic elements such as a firewall and access control. In addition ACS Law's web-hosting package was only intended for domestic use. Mr Crossley had received no assurances from the web-host that information would be kept secure. While the firm should have been aware of their obligations under the Data Protection Act, they continued to act negligently and failed to ensure that appropriate technical and organisational measures were in place to keep personal information secure.

ENDS

If you need more information, please contact the ICO press office on 0303 123 9070 or visit the website at: www.ico.gov.uk.

Notes to Editors

1. The monetary penalty served on Andrew Jonathan Crossley is available on the ICO website here: http://www.ico.gov.uk/~/media/documents/library/Data_Protection/Notices/acs_law_monetary_penalty_notice.pdf

2. The Information Commissioner's Office upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

3. The ICO has specific responsibilities set out in the Data Protection Act 1998, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Privacy and Electronic Communications Regulations 2003.

4. For more information about the Information Commissioner's Office subscribe to our e-newsletter at www.ico.gov.uk. Alternatively, you can find us on Twitter and Linkedin.

5. Anyone who processes personal information must comply with eight principles of the Data Protection Act, which make sure that personal information is:
    - Fairly and lawfully processed
    - Processed for limited purposes
    - Adequate, relevant and not excessive
    - Accurate and up to date
    - Not kept for longer than is necessary
    - Processed in line with your rights
    - Secure
    - Not transferred to other countries without adequate protection