Carphone Warehouse fined £400,000 after serious failures placed customer and employee data at risk

Date
10 January 2018

Type
News

Carphone Warehouse has been issued with one of the largest fines by the Information Commissioner's Office (ICO), after one of their computer systems was compromised as a result of a cyber-attack in 2015.

The company's failure to secure the system allowed unauthorised access to the personal data of over three million customers and 1,000 employees.

The compromised customer data included: names, addresses, phone numbers, dates of birth, marital status and, for more than 18,000 customers, historical payment card details.

The records for some Carphone Warehouse employees, including name, phone numbers, postcode, and car registration were also accessed.

The ICO considered that the personal data involved would significantly affect individuals' privacy, leaving their data at risk of being misused.

Information Commissioner Elizabeth Denham said:

> "A company as large, well-resourced, and established as Carphone Warehouse, should have been actively assessing its data security systems, and ensuring systems were robust and not vulnerable to such attacks.
>
> "Carphone Warehouse should be at the top of its game when it comes to cyber-security, and it is concerning that the systemic failures we found related to rudimentary, commonplace measures."

Warehouse's approach to data security and determined that the company had failed to take adequate steps to protect the personal information.

Using valid login credentials, intruders were able to access the system via an out-of-date WordPress software.

The incident also exposed inadequacies in the organisation's technical security measures. Important elements of the software in use on the systems affected were out of date and the company failed to carry out routine security testing. There were also inadequate measures in place to identify and purge historic data.

The ICO considered this to be a serious contravention of Principle 7 of the Data Protection Act 1998.

The Commissioner acknowledges the steps Carphone Warehouse took to fix some of the problems and to protect those affected. She also acknowledges that to date there has been no evidence that the data has resulted in identity theft or fraud.

Ms Denham said:

> "The real victims are customers and employees whose information was open to abuse by the malicious actions of the intruder.
>
> "The law says it is the company's responsibility to protect customer and employee personal information.
>
> "Outsiders should not be getting to such systems in the first place. Having an effective layered security system will help to mitigate any attack – systems can't be exploited if intruders can't get in.
>
> "There will always be attempts to breach organisations' systems and cyber-attacks are becoming more frequent as adversaries become more determined.
>
> "But companies and public bodies need to take serious steps to protect systems, and most importantly, customers and employees."

From 25 May this year, the law is set to get more stringent as the General Data Protection Regulation (GDPR) comes into effect. Data protection by design is one of the requirements and must be in every part of information processing, from the hardware and software to the procedures, guidelines, standards, and polices that an organisation has or should have.

> nies and public bodies should ensure strong IT governance and information security es are in place, tested and refreshed to comply with the provisions of the law.

the steps organisations can take to protect themselves.

Notes to Editors

1. The Information Commissioner's Office upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
2. 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.
3. The ICO can take action to change the behaviour of organisations and individuals that collect, use and keep personal information. This includes criminal prosecution, non-criminal enforcement and audit. The ICO has the power to impose a monetary penalty on a data controller of up to £500,000.
4. The ICO fined TalkTalk £400,000 in October 2016 after security failings that allowed a cyber attacker to access customer data.
5. The European Union's General Data Protection Regulation (GDPR) is a new law which will apply in the UK from 25 May 2018. The Government has confirmed the UK's decision to leave the EU will not affect the commencement of the GDPR. The Government is introducing measures related to this and wider data protection reforms in a Data Protection Bill.
6. 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; and
    - not transferred to other countries without adequate protection.
7. Civil Monetary Penalties (CMPs) are subject to a right of appeal to the (First-tier Tribunal) General Regulatory Chamber against the imposition of the monetary penalty and/or the amount of the penalty specified in the monetary penalty notice.
8. Any monetary penalty is paid into the Treasury's Consolidated Fund and is not kept by the Information Commissioner's Office (ICO).

eport a concern to the ICO telephone our helpline 0303 123 1113 or go to
org.uk/concerns.

Subscribe to our e-newsletter

The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.