Client Update

UK Telecoms Retailer Fined for Data Security Failures – What Can Others Learn?

UK TELECOMS RETAILER FINED £400,000 FOR DATA SECURITY FAILURES – WHAT CAN OTHERS LEARN?

On 8 January 2018, the Information Commissioner's Office (ICO) fined leading telecoms retailer Carphone Warehouse £400,000 for having inadequate technical and organisational measures to safeguard employee and customer personal data. The ICO's Penalty Notice provides useful guidance to companies on technical and organisational safeguards they may be expected to have in place to secure personal data. With higher potential penalties for such failures under the forthcoming EU General Data Protection Regulation ("GDPR"), businesses handling personal data should consider whether their safeguards and controls suffer from any of the deficiencies for which the ICO fined Carphone Warehouse.

Why did the ICO fine Carphone Warehouse?

Between 21 July and 5 August 2015, attackers apparently targeted a collection of Carphone Warehouse's virtual servers which hosted internal and external websites. The ICO Penalty Notice reveals that the system housed a large volume of personal data: over 3.3 million customer records, historic payment details for over 18,000 payment cards and approximately 1,000 employee records.

According to the ICO, the attackers scanned the system with a penetration testing tool to identify vulnerabilities. The attackers then seemingly gained access to the system either by using vulnerabilities in an outdated content management system or valid administrator credentials from an unknown source. Having gained access to the system, the attackers had — at a minimum — access to a large volume of personal data, with indications that some of it may have been exfiltrated. Carphone Warehouse apparently became aware of the breach and began to take remedial steps on 5 August 2015 when unauthorized decryption activity was detected and raised the alarm.

Having investigated the incident after Carphone Warehouse self-reported, the ICO determined that the company's safeguards had "multiple, systemic and serious inadequacies" which merited the £400,000 monetary penalty.

What could Carphone Warehouse have done better?

In its Penalty Notice, the ICO identified organisational and technical failings that it considered to constitute breaches of Carphone Warehouse's data protection obligations. Notably, the ICO reached this view irrespective of whether the specific failings contributed to the data breach. Those failings, along with key takeaways for companies, are noted below.

- *Out-of-date software*. The ICO identified that key elements of the system's software were significantly out of date. Despite having a "Patch Management Standard" in place, Carphone Warehouse did not follow it. This lapse resulted in what the ICO felt were serious, and avoidable, vulnerabilities. Likewise, contrary to the company's policy, anti-virus software was not installed on the relevant servers. While paper compliance in the form of written procedures and manuals is important, companies should consider conducting periodic reviews of their processes to ensure that their written policies are followed in practice. If there are good reasons for deviating from those policies, then deviations should be formally approved and their rationale recorded.
- *Inadequate credential management*. The ICO found that Carphone Warehouse failed to adequately manage login credentials. The company had no credential misuse detection system and the root password for several server operating systems was the same and known to 30-40 employees. Companies should limit access (and, in particular, administrator-level access) to systems containing personal data and have measures in place to detect misuse of valid credentials. This can help increase the prospects of early incident detection and mitigate damage.
- *No Web Application Firewall ("WAF")*. It appears from the Penalty Notice that when the attack occurred, Carphone Warehouse did not have a WAF to monitor and filter traffic to and from its web applications. While it was unclear whether a WAF would have prevented the attack, the ICO identified this as a significant failing and its absence contrary to accepted industry security practice. Beyond the benefits of a WAF, the ICO's comments suggest that companies should routinely revisit their security infrastructure to ensure that it meets industry standards as technologies advance and best practices evolve.
- *Insufficient vulnerability and penetration testing*. The ICO discovered that Carphone Warehouse had not performed routine testing procedures, such as internal or external penetration testing, in the 12 months preceding the attack. This indicates that the ICO, like many other regulators, views annual penetration testing as a practice that may be required to comply with the obligation to implement adequate measures to safeguard personal data. Notably, Carphone Warehouse's policy called for annual testing but the policy was not followed.

- *Over-inclusive and unsecure data retention*. The ICO found that the compromised systems held old transaction data including credit card details for no good reason; in fact, Carphone Warehouse apparently acknowledged that it did not know the data had been retained on the system. Moreover, although the data were encrypted, the decryption keys were stored in plain text in the application's source code, and were therefore easily accessible to hackers. Data minimisation — that is, storing personal data for no longer than is necessary — is a key data protection requirement, and companies need to implement processes to keep track of what data they hold and purge it when it is no longer needed. Where personal data are retained, they have to be stored securely, and encryption should meet prevailing industry standards and be updated as they evolve.

THE FUTURE UNDER THE GDPR

While the fine may be the same size as the one that the ICO gave TalkTalk in 2016, the ICO's Penalty Notice is notable for the greater depth in which it addresses Carphone Warehouse's technical failures; perhaps signaling that the ICO will, in the future, subject companies' technical safeguards to greater scrutiny. Lessons that other companies learn from Carphone Warehouse's experience will also become increasingly important in May 2018, when the GDPR comes into force. Not only does the GDPR significantly increase fines for non-compliance, but it also engages with technical security requirements in much greater detail than the current Data Protection Directive. It is therefore likely that, as time goes on, EU Data Protection Authorities will increase their focus on technical safeguards, as the ICO had done in this case. Companies should consider getting ahead of this trend by taking steps to improve their data security procedures and controls and ensure that those procedures and controls are followed in practice.

Debevoise advises businesses, both in and outside of the European Union, on all aspects of GDPR and cybersecurity preparedness and breach response.

* * *

Please do not hesitate to contact us with any questions.

NEW YORK
Jeremy Feigelson
jfeigelson@debevoise.com

Jim Pastore
jjpastore@debevoise.com

LONDON
Jane Shvets
jshvets@debevoise.com

Robert Maddox
rmaddox@debevoise.com