Client Alert: PC World owner fined after data breach

Date : January 9, 2020

Today the UK Data Protection Authority, the Information Commissioner's Office (ICO), announced that it had fined DSG Retail Ltd, the owner of a number of well-known retailers including PC World, £500,000 after a data breach.

It is important to remember that this is a fine under the Data Protection Act 1998 (DPA 1998) the previous data protection regime which existed prior to the coming into force of GDPR and the Data Protection Act 2018 (DPA 2018) in May 2018. £500,000 was the maximum fine permitted under the old data protection regime.

What happened?

DSG's systems were compromised between July 2017 and April 2018 by a hacking attack. DSG learned of the breach in April 2018 after what the ICO called "*external intelligence*" alerted it to the vulnerability in its systems.

A subsequent investigation found malware installed on 5,390 point of sale (EPOS) terminals. In simple terms EPOS terminals are what used to be known as tills in stores. The malware on the EPOS systems meant that the attacker could intercept card details from the EPOS terminals used in DSG stores. Whilst DSG was unable immediately to work out the amount of data compromised, it subsequently told the ICO that around 5.6m payment cards were affected. In addition other records of 14m people may have been compromised. DSG argued that for technical reasons the breach was not as large as this might suggest as it felt some data was anonymised. The ICO disagreed with that. The Monetary Penalty Notice (MPN) which explains the ICO's reasoning has more detail on that. In our experience it is often the case that people fail to understand the true meaning of anonymisation under data protection law. Our data protection glossary here explains the difference between anonymisation and pseudonymisation www.bit.ly/gdprwords

What did the ICO say?

The ICO took action under the security provisions of DPA 1998 saying that DSG did not have adequate technical and organisational measures (TOMs) in place to protect personal data. This part of DPA 1998 is essentially the same in GDPR and DPA 2018 and so the ICO's reasoning in the DSG case is useful when looking at the new regime as well. The ICO makes it clear in the MPN that the fine against DSG would have been higher had this been a GDPR breach.

Steve Eckersley, Director of Investigations at the ICO said:

"Our investigation found systemic failures in the way DSG Retail Limited safeguarded personal data. It is very concerning that these failures related to basic, commonplace security measures, showing a complete disregard for the customers whose personal information was stolen. The contraventions in this case were so serious that we imposed the maximum penalty under the previous legislation, but the fine would inevitably have been much higher under the GDPR."

What has DSG said?

DSG says that it previously made representations to the ICO prior to the fine being announced and that it is considering an appeal. It called the breach "*historic unauthorised access*". DSG's CEO Alex Baldock, said: "*We are very sorry for any inconvenience this historic incident caused to our customers. When we found the unauthorised access to data, we promptly launched an investigation, added extra security measures and contained the incident. We duly notified regulators and the police and communicated with all our customers. We have no confirmed evidence of any customers suffering fraud or financial loss as a result. We have upgraded our detection and response capabilities and, as the ICO acknowledges, we have made significant investment in our Information Security systems and processes*."

What are the lessons learned?

The MPN is a long and technical document but is certainly worth a read for anybody involved in retail security and EPOS systems in particular. There are lessons to be learned across the fore however which include:

1. Businesses need to understand the difference between anonymised and pseudonymised data. Truly anonymised data that is useful is in our experience very rare. The failure to understand the differences between anonymised and pseudonymised data can have dramatic consequences.
2. Organisations need to make sure that they properly monitor their networks. This will include having measures in place to detect unusual activity but also to predict vulnerabilities. It is often a feature of data protection cases that hackers exploit known vulnerabilities and that is the case here. Organisations need to make sure that all of the software is patched properly and promptly.
3. Organisations need to respond quickly to vulnerabilities. Here the ICO said that some of the issues had been highlighted in an earlier PCI DSS audit and these issues were not remedied in time. Since this was a pre-GDPR case the ICO did not look at the 72 hour reporting limit but it is clear that since GDPR came in organisations have even less time to respond to issues.
4. Organisations need to be geared up to help victims if they do have an issue. In this case the ICO took into account the fact that DSG reached out to 25m potential victims, it took out an advertisement to let people know about the breach and it proactively told the ICO. The ICO also took into account the fact that DSG set up a dedicated call centre, offered credit monitoring to victims and started a program of working with banks to minimise harm. The ICO said however that it gained limited credit for these measures as they were now "*industry standard*". It is clear that particularly for B2C businesses measures like this will be necessary when there is a breach.
5. When there is an incident organisations will need to make sure that they can keep potential victims informed and happy. In setting the fine the ICO took into account the fact that they had received 258 complaints and that DSG had 3,303. The extracts from some of the complaints to ICO were included in the MPN – it is clear that the ICO will take customer sentiment into account when deciding on aggravating and mitigating factors in a breach.
6. Organisations need to understand that even if they have the best TOMs in place breaches are inevitable. They have to invest in proper processes and procedures to deal with data breaches. Rehearsals like our Data Breach Academy can help https://www.corderycompliance.com/cordery-data-breach-academy-2-2/ and systems like Cordery Breach Navigator can help an organisation respond.

There are details of Cordery Breach Navigator here https://www.corderycompliance.com/solutions/breach-navigator/.

There are some tips on handling data breaches here https://www.corderycompliance.com/dealing-with-a-data-breach/

There is more information about this and other data protection topics in Cordery's GDPR Navigator subscription service. GDPR Navigator includes short films, straightforward guidance, checklists and regular conference calls to help you comply. More details are at www.bit.ly/gdprnav.

You can see more details of the case and the Monetary Penalty Notice issued b the ICO here http://bit.ly/2FBzicl.

For more information please contact Jonathan Armstrong or André Bywater who are lawyers with Cordery in London where their focus is on compliance issues.

Jonathan Armstrong
Cordery
Lexis House
30 Farringdon Street
London EC4A 4HHOffice: +44 (0)20 7075 1784
jonathan.armstrong@corderycompliance.com

Andre Bywater
Cordery
Lexis House
30 Farringdon Street
London EC4A 4HHOffice: +44 (0)20 7075 1785
andre.bywater@corderycompliance.com