Summary Final Decision Art 60

Legal obligation

Administrative fine

EDPBI:UK:OSS:D:2020:147

Background information

Date of final decision:	16 October 2020
Date of broadcast:	16 October 2020
LSA:	UK
CSAs:	All SAs
Legal Reference:	Personal data breach (Articles 33 and 34), Security of processing (Article 32)
Decision:	Administrative fine
Key words:	Administrative fine, Data security, Hacker attack, Personal data breach, Credentials

Summary of the Decision

Origin of the case

On 22 June 2018, the unidentified attacker gained access to controller's IT systems via CAG (a tool that allows users to remotely access a network) and maintained this ability to access undetected until 5 September 2018.

After gaining access to the wider network, the attacker traversed across the network. This culminated in the editing of a Javascript file on the controller's website. The edits made by the attacker were designed to enable the exfiltration of cardholder data from that website to an external third-party domain, which was controlled by the attacker.

The controller was alerted by a third party about the exfiltration of personal data from the controller's website and then notified the LSA about the attack on 6 September 2018.

The controller estimated that 429,612 data subjects were affected. The affected categories of personal date were: username and passwords of contractors, employees and members of the Executive club, customer names and addresses, unencrypted payment card data including card numbers, and CVV numbers and expiry dates.

The controller took immediate measures to mitigate and minimise any damage suffered by the data subjects by implementing remedial measures, including notifying banks and payment schemes, the data subjects and data protection regulators; cooperating with regulatory and governmental bodies; and offering a reimbursement to all customers who had suffered financial losses as a direct result of the theft of their card details.

The controller also implemented a number of remedial technical measures to reduce the risk of a similar attack in future.

Findings

The LSA found that the controller failed to process the personal data of its customers in a manner that ensured appropriate security of the data, including: protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures, as required by Article 5(1)(f) and by Article 32 GDPR.

The LSA concluded that there are a number of appropriate measures that the controller could have considered to mitigate the risk of an attacker being able to access the controller's network. The LSA considered that each step of the attack could have been prevented, or its impact mitigated, by the controller's implementing one or more of those appropriate measures that were open to controller. The LSA also considered that, had the controller performed more rigorous testing or internal penetration tests, it would have likely detected and appropriately addressed many of the data security problems identified.

Decision

The LSA concluded that the infringements constitute a serious failure to comply with the GDPR. The LSA decided to impose on the controller an administrative fine of £20 million, after having taken into account a range of mitigating factors and the impact of the Covid-19 pandemic.