

# Summary Final Decision Art 60

Legal obligation

Administrative fine

EDPBI:UK:OSS:D:2020:154

## Background information

Date of final decision:	13 November 2020
Date of broadcast:	16 November 2020
LSA:	UK
CSAs:	All SAs
Legal Reference:	Articles 33 and 34 - Personal data breach
Decision:	Administrative fine
Key words:	Personal data breach

## Summary of the Decision

### Origin of the case

The personal data breach in the case at stake related to exposed personal details, such as names, payment card numbers, expiration dates and CVV numbers. 9.4 million EEA data subjects, of whom 1.5 million in the UK, were notified as having been potentially affected by the personal data breach. The personal data breach related to compromised bankcard details and transaction fraud on bank accounts. One bank advised that around 60.000 individuals' card details had been compromised, while another bank recommended that around 6.000 payment cards be replaced as result of controller's transaction fraud. The controller received around 997 complaints by individuals', claiming economic loss and/or emotional distress. The controller was not able to provide to the SA a detailed analysis of the individuals affected.

### Findings

The LSA found that the controller had failed to process personal data in a manner that ensured appropriate security of the personal 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 Article 32 GDPR. In addition, the LSA found that the controller failed to detect and remediate the breach in a timely manner or provide a fully

detailed analysis of the individuals affected to the LSA within 72 hours after having detected the personal data breach. Furthermore, the LSA considered mitigation factors, such as the fact that the controller forced password resets across all its domains and created a website where customers could access to information about the personal data breach.

### Decision

In view of the above, the LSA imposed an administrative fine on the controller of £1,250,000.00.