Summary Final Decision Art 60

Data breach notification

No sanction

EDPBI:UK:OSS:D:2020:100

Background information

Date of broadcast:	15 April 2020
LSA:	UK
CSAs:	BE, DE, EE, IE, EL, ES, FR, IT, HU, NL, PL, SI, SK, FI
Legal Reference:	Principles relating to processing of personal data (Article 5), Security of Processing (Article 32); Notification of a personal data breach to the supervisory authority (Article 33)
Decision:	No sanction
Key words:	Personal data breach, Remediation measures

Summary of the Decision

Origin of the case

On 21 August 2019, the controller reported a data breach to the LSA related to a payment infrastructure that enabled near real-time payments between bank accounts of the regional financial institutions.

The breach concerned an identifier linked by a customer to one of their bank accounts that can be provided to others to receive payments into the linked bank account) enumeration attack against a financial institution and their sponsor. The infrastructure included a feature that prompted an identifier lookup at the sponsor's addressing service feature whenever customers entered an identifier into the payee field in an online banking facility. Customers then would have displayed the identifier name registered with the introduced identifier, helping them to reduce the risk of payments to unintended recipients. The financial sponsor identified a larger than normal number of an identifier enquiries, and subsequent investigations led them to identify a vulnerability in their identifier lookup service.

Findings

The individual and organisation customer names, mobile phone numbers and the associated account numbers and BSB (Bank /State /Branch) number had been exposed by the breach. The LSA found that this was not a breach of the controller's systems, rather the processor's systems. The LSA also established that the exposed data could not be used to access a bank account by itself.

The breach affected thousands of individuals, a number of which were identified as customers of the controller and identified as being EU citizens.

The LSA found that the breach had caused low detriment to individual data subjects. The controller took steps to notify affected data subjects and heightened monitoring on the affected accounts to look for any signs of fraudulent activity, as well as offered them an independent enhanced fraud detection identification and cyber-monitoring service for free.

Decision

The LSA considered that whilst a data breach had occurred, and individual data subjects were affected, the breach did not meet the threshold for regulatory action due to the low number of affected EU data subjects and the post-incident actions taken by the controller to remediate the situation, which had reduced the risk of fraudulent activity on customers' accounts.

The LSA decided that no further action should be taken and closed the case.