THE TIMES

business

RBS hides Natwest data breach from customers

James Hurley, Enterprise Editor
561 words
19 August 2019
01:47
thetimes.co.uk
TIMEUK
English

Highly sensitive personal data, including banking details of more than 1,600 Natwest customers, has been left in a former employee's home for more than a decade because the bank has been unable to reach an agreement on the safe return of the information.

Royal Bank of Scotland,

Natwest

's owner, has not alerted affected customers to the serious data breach because it does not know exactly what information its former worker holds.

Anonymous examples seen by

The Times

suggest that the information includes account and sort codes, credit card details and people's account histories, including direct debits, as well as their names, addresses, relationship status, occupation and phone numbers.

The former Natwest employee, who was dismissed by the bank in June 2009, said she had been trying to negotiate the safe return of the information ever since.

The bank worker, who spoke on condition of anonymity, sold financial products to consumers and small business owners. She claims she was sacked after raising concerns about the security of her home working arrangement. A claim for unfair dismissal was unsuccessful.

The Information Commissioner's Office, the data regulator, subsequently confirmed there had been a data security breach in the case after she alerted the ICO to the issue.

Rules which came into force in May 2018 mean organisations have a responsibility to "inform individuals without undue delay" in the case of serious data breaches.

A breach can be a "security incident that has affected the confidentiality, integrity or availability of personal data", the ICO says. Organisations must notify the ICO within 72 hours of becoming aware of a personal data breach.

The RBS breach, however, pre-dates these rules and the ICO confirmed the incident took place "under previous data protection legislation, when there was no mandatory reporting requirement".

A planned meeting last month between the individual and the bank was cancelled after negotiations with Ross McEwan, the RBS chief executive, broke down when he was given the impression the former employee wanted to retain a copy of the information, in the bank's view rendering any exchange pointless.

The former worker says she wanted to temporarily retain copies to protect her own legal position and also because she plans to show them to the Financial Conduct Authority to highlight alleged mis-selling issues.

She said she is now happy to return the information if RBS provides written confirmation that the data matches a schedule she will produce, at which point remaining copies will be given to the ICO and the FCA.

A meeting would “give the bank the opportunity to see the documents, understand the nature of the content and alert affected customers”, she said. “I still hope to find a way forward with RBS to return the data in a secure manner.”

RBS is understood to view the data as “historic” in nature and does not plan to take legal action to recover it. The bank indicated it remains in negotiations to arrange its safe recovery.

An ICO spokesperson said it had “provided advice on data protection issues to parties involved an employment dispute dating back to 2009.” It added: “We are satisfied that the potential risk posed to individuals does not warrant further action, despite there being a change in the law (GDPR) since that time.”

Document TIMEUK0020190818ef8i0003c

