VERDICT

Robert Scammell – 6th August 2019 11:22AM

Monzo has told some 500,000 of its customers to change their personal identification number (PIN) after the challenger bank incorrectly stored them in its own internal systems.

The digital bank said that it had inadvertently copied around a fifth of UK customers' PINs to encrypted log files. These log files could only be accessed by Monzo engineers and were stored for up to six months in this location.

Monzo became aware of the PIN breach on Friday and rolled out an update to the app the following day. By Monday it had deleted the

incorrectly stored data and sent an email to those affected asking them to change their pin. Monzo also recommends that customers update to the latest version of the app.

Monzo said that nobody outside of the bank had access to the PINs and that there is no evidence that the information has been used to commit fraud.

“We’ve checked all the accounts that have been affected by this bug thoroughly, and confirmed the information hasn’t been used to commit fraud,” Monzo said in a blog post.

“Just in case, we’ve messaged everyone that’s been affected to let them know they should change their pin by going to a cash machine.”

Jake Moore, cybersecurity specialist at ESET, said:

“If a bank tells you to change your PIN then things are not going very well. In an ideal world, not even the engineers should have had access to the codes, which would have mitigated this problem.

“But then again, like any breach, most never think it will ever happen. Obviously, changing your PIN number is advised, but if all of your cards use the same PIN, it would be best practice to change them too – just like in a password breach.”

Did the Monzo PIN error breach GDPR?

Monzo appears to have reported the breach to the Information Commissioner’s Office, the UK’s data regulator, within the 72 hour period stipulated under the General Data Protection Regulation.

The ICO told the Financial Times: “We are aware of an incident involving Monzo and we will be assessing the matter.”

Robert Wassall, director of legal services for cybersecurity firm ThinkMarble, told Verdict that the Monzo PIN breach is something the ICO would “likely be very concerned about” because it involves a financial institution.

Wassall pointed out that 500,000 customers is a similar number of people compromised in the

British Airways breach, for which the ICO recently levied a record £183m GDPR fine. BA fell victim to a cyberattack in which hackers stole payment details from the company's website.

The airline fell afoul of the 'Breach of Principle of Integrity and confidentiality', a key GDPR principle that requires organisations to uphold appropriate technical and organisational measures to process personal data securely.

Wassall said that the Monzo PIN breach would likely fall under the same principle.

In a May blog post, information commissioner Elizabeth Denham said the ICO would be focusing on this principle for the second half of 2019:

"Organisations need to shift their focus to accountability with a real evidenced understanding of the risks to individuals in the way they process data and how those risks should be mitigated," she wrote.

Jasmit Sagoo, senior director, head of technology UK & Ireland at Veritas, an enterprise data protection firm, said:

“Poor data hygiene is bad for business, threatening the foundation of the customer relationship and the organisation itself.

“Leaving data disorganised also makes it vulnerable, opening it up to potential bad actors and exponentially increasing the chances of a highly damaging data breach. Sensitive customer information –bank details or home addresses – is then ripe for the taking if poorly protected.

“Good data hygiene is not easy to achieve, but it’s increasingly necessary. To compete in a marketplace where trust is a valued commodity, businesses must prove they are responsible with customer data and meet their data requirements.”

The Monzo PIN breach comes at a time when the bank is looking to expand into the US.

The bank, which has no physical branches, is currently valued at £2bn.