DRN-4399415

The complaint

Mr B complains that PRA Group (UK) Limited (PRA) sent him an email saying that his data had been compromised.

Mr B wants PRA to compensate him for the resulting distress and uncertainty.

What happened

PRA uses a third party business to transfer personal data. In 2023, the third party was the subject of a cyber-attack which impacted many of its customers, including PRA.

When our investigator first considered Mr B's complaint, he thought that as PRA decided to use a third party to transfer data, PRA needed to ensure that it had appropriate protections in place. As our investigator didn't think that PRA had shown what steps it took to protect the data, he thought PRA was responsible for the impact of the data breach on Mr B.

Our investigator noted that Mr B hadn't yet suffered any financial loss because of the breach but could understand his concern that something may happen in the future. Our investigator asked PRA to pay Mr B £250 and offer a free protective fraud marker for the next two years.

Mr B was happy with the investigation outcome but PRA disagreed. PRA acknowledged that it was the data controller of Mr B's personal data. PRA explained that it had used the third party business for several years. PRA said that the third party was a leading business in its field but that it had been the subject of a sophisticated cyber-attack which had impacted hundreds of global and national organisations.

PRA explained that as well as using a secure managed file transfer application, it also employs a wide range of security methods. PRA detailed some of these measures on a confidential basis.

PRA said that it reported the data breach to the Information Commissioner's Office (ICO) and set out what remedial steps it had taken to further protect customers. PRA also made a voluntary notification to the Financial Conduct Authority (FCA). Neither the ICO nor the FCA raised concerns about the way that PRA handled the incident.

PRA set out further details of the steps it had taken in response to the cyber-attack, including taking legal advice and forming a specific team to follow up with customers.

PRA said that it might not always be helpful for customers to sign up to fraud prevention services as having a marker against their name may negatively impact future lending applications. PRA recommended that customers continue to use a free credit monitoring service.

Finally, PRA thought the proposed compensation was excessive as there had been no financial loss to Mr B and PRA had acted in line with its regulatory requirements.

After considering everything again, our investigator issued a second investigation outcome. In light of the information PRA had provided, our investigator thought PRA had put

appropriate security measures in place and was not at fault for the breach.

Our investigator suggested that Mr B could take his concerns about the data breach to the ICO but that as things stood, our investigator couldn't hold PRA responsible. This meant he no longer thought it fair to require PRA to pay compensation or cover the cost of a protective fraud marker.

Mr B is unhappy with the second investigation outcome. He can't see why PRA wants to quibble about paying £250. Mr B says it's strange that PRA think the Financial Ombudsman wasn't the appropriate organisation to be involved in his complaint given PRA referred him to our service in its final response.

What I've decided – and why

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

I realise that I've summarised this complaint in less detail than the parties and I've done so using my own words. I've concentrated on what I consider to be the key issues, particularly as our investigator has already given Mr B a detailed explanation of why he no longer thinks that PRA is to blame. The rules that govern this service allow me to do so. But this doesn't mean that I've not considered everything that both parties have given to me

To answer Mr B's query about why PRA referred to the Financial Ombudsman in its final response - PRA is regulated by the FCA and has to follow the FCA's complaint handling rules, which include providing referral rights to the Financial Ombudsman.

It's not the role of the Financial Ombudsman to decide if a business has breached data protection laws – that falls to the ICO to decide. And we can't regulate or discipline the businesses that we cover. We can however consider whether a business should compensate a consumer where it has made a mistake and the mistake relates to a regulated activity that we are allowed to consider under the rules that govern our service.

I fully understand Mr B's frustration with the fact that our investigator had a change of view but I can't see that PRA is responsible for the data breach. The evidence which PRA has provided – some of which I can't share because of its commercial sensitivity – shows that it has suitable protections in place to ensure personal data is kept safe.

Once PRA became aware of the data breach, it acted quickly to notify the ICO and then follow the guidance released by the ICO on its website. PRA has today told this service that the ICO has confirmed that it is not taking any regulatory action against PRA following the breach. The ICO says that this is due to the particular facts of the case and the remedial measures that PRA set out in its report.

I'm satisfied that PRA promptly notified Mr B so that he in turn could take his own steps to protect his data. I consider PRA took all reasonable steps to minimise any potential risks to Mr B.
I don't want to in any way downplay the distress and upset that Mr B has felt after learning about the breach. I can understand his concern and uncertainty over the security of his data. But as I'm not persuaded that PRA did anything wrong, I don't consider it fair to award compensation or ask PRA to pay for the protective marker service.

Our investigator has already explained to Mr B what steps he can take to monitor his personal and credit information in the future. I leave this with Mr B to action if he chooses.

My final decision

My final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr B to accept or reject my decision before 21 November 2023.

Gemma Bowen
Ombudsman