DRN-4111725

The complaint

Mr P complains that Sainsbury's Bank Plc are holding him liable for credit card transactions he says he didn't make. He'd like the transactions refunded.

What happened

Mr P has appointed representatives for this complaint – but for ease of reading I'll refer solely to Mr P in this decision.

Mr P held a credit card account with Sainsbury's. In February 2021 he contacted the bank to discuss his finances. He later carried out a balance transfer to a different credit card provider. Later that month the address on the account was amended by phone call to a different area of the country. A new card and PIN were ordered and delivered to the new address.

In late March 2021 there were four large transactions on the account totalling £6,676.65. Mr P says he first became aware of them when he received a text message telling him he was close to his limit. He contacted Sainsbury's to say he hadn't made these transactions and shouldn't be held responsible.

Sainsbury's looked into what happened but declined to refund the payments. They couldn't see how an unknown third party could have gathered enough information to pass security without Mr P's involvement.

Mr P later found that Sainsbury's had registered a marker with the fraud prevention agency CIFAS against him. He complained about this, but Sainsbury's said they were satisfied with the information they'd recorded.

Unhappy with this Mr P referred his complaint to our service. One of our investigators looked into what happened but didn't think Sainsbury's needed to do anything further. They accepted that the caller's voice on the calls to Sainsbury's was different to Mr P. But they said they couldn't see how the person who called would have known enough personal information about Mr P to pass security.

The investigator saw that Mr P had accessed his online account after the address had changed, so thought he ought to have noticed this. They also couldn't see a reason why a fraudster who had ordered a new card would wait almost a month before attempting to use it. The locations of the disputed usage were closer to Mr P's actual address than the changed address.

Overall, the investigator felt it likely that the transactions were authorised by Mr P himself, or someone with his knowledge and consent.

Mr P disagreed, saying the information used to pass security could have come from other sources, or be obvious to answer. But this didn't change the investigator's mind. As no agreement could be reached, the complaint was passed to me to decide. On review of the

evidence I reached broadly the same conclusions as the investigator and issued my provisional decision which said the following.

Reviewing the technical evidence, it's clear to me the payments were made using a card issued and verified using the PIN. The key consideration for me here is whether I think it's more likely than not the transactions were carried out either by Mr P, or someone with his authorisation to do so. The relevant regulations say that Sainsbury's can only hold him liable for the transactions if this is the case.

Having considered everything, I'm minded that it's reasonable to conclude Mr P was involved in the transactions. There are several points that lead me to this conclusion:

- *I don't have a copy of the call where the new card was ordered, but I do have the calls where the account address was updated, and a new PIN was ordered. These are made by someone with a different voice to Mr P. However, I do find it unusual that the caller updates the address but makes no attempt to update any other contact details such as the telephone number or email address. I might expect a fraudster to do this, so they can gain full control of the account.*
- *The caller passes the additional security questions without any difficulty, which shows me that they had considerable knowledge of Mr P. The additional security involved other parties Mr P held accounts with and his energy provider. In the call the bank state the additional questions came from information on Mr P's credit file, so it's possible that they could have obtained the information from there. But I've not received any indication that Mr P's data had been compromised by any third party.*
- *The new PIN was issued on 7 March, but the first payment doesn't take place until 27 March. It doesn't seem likely to me that a fraudster, in possession of the card and PIN, would wait several weeks before attempting any transactions. They wouldn't be aware of when the cardholder would discover the change of address, or that a new card had been issued. So, I may expect them to try and make use of all the available funds as quickly as possible. The delay before attempting any transactions suggests they were aware the card would still be usable.*
- *The transactions take place over four days, which again suggests there was no rush to use the available balance. There were no further attempts to use the card after it was cancelled, which suggests whoever had the card knew it wouldn't work any further.*
- *The online banking for the card is accessed several times between the address being changed and the transactions in dispute. There is no suggestion Mr P's online banking details had been compromised – he had recently changed the password, and to do so required two-factor authentication. Mr P had said he was checking that a balance transfer had gone through, but this had been completed several weeks prior. This doesn't seem a likely explanation to me. The statements were accessed at one point, which would have shown the updated address. If Mr P hadn't expected this I may have expected him to report this to Sainsbury's at the time.*
- *The places the card was used are significantly closer to Mr P's address than the updated address. While I accept Mr P's point that the transactions could have taken place anywhere, I don't think it likely a fraudster would choose to travel several hundred miles to make large transactions rather than carry them out more locally.*

Take all of this into account, I don't see it likely that the transactions were carried out by some unknown third party. While there's no typical fraudster, I would generally expect a fraudster to act as quickly as possible. But in this case whoever was accessing the account seemed particularly unhurried – which for a fraudster would expose them to much greater risk they'd be found out. The only plausible explanation I can see is that the transactions

were carried out either by Mr P, or someone with his authorisation. On that basis, it's not unreasonable for Sainsbury's to hold him liable for them, and to ask that they be repaid.

Sainsbury's have also recorded a marker with the fraud prevention agency CIFAS. There are certain standard of evidence a business needs to be able to evidence to record a marker with CIFAS – that there is evidence fraud or financial crime took place or was attempted and that the person the marker is about was complicit. The evidence needs to be clear and rigorous and need to go beyond mere suspicion.

I've considered this point carefully. In this case I'm satisfied for the reasons above that Mr P was involved in the transactions reported as fraudulent. And I'm satisfied that the totality of evidence Sainsbury's hold meets the standard set out in CIFAS. Therefore, it's not unreasonable for this marker to be reported.

Sainsbury's accepted the provisional decision. Mr P disagreed, saying the conclusions reached were not a reasonable assessment of the complaint. He said the provisional decision was based on assumptions of what a typical fraudster would do, despite the decision saying there is no typical fraudster. He said he had been the victim of a sophisticated fraud. He felt the burden of proof for any compromise of his personal data should fall on Sainsbury's. He felt the findings that he was involved were irrational, and the evidence he'd provided hadn't been given due weight.

Mr P provided emails he says show he was working at the time of the fraudulent transactions. These were shared with Sainsbury's, but this didn't change their mind. I've now reconsidered all the available evidence, along with the additional points raised by Mr P.

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.

Having done so, I remain satisfied with the conclusions reached in my provisional decision.

In his response to the provisional decision Mr P commented that he believes a court would find in his favour, because he claims there is a lack of evidence that he was involved in the transactions. As he has acknowledged though our service isn't a court and isn't intended to replicate what a court does – our remit is to resolve complaints quickly and informally, based on what the ombudsman considers to be fair and reasonable in the circumstances of the complaint.

In considering this complaint I've taken in to account the relevant legislation and regulations – including the Payment Services Regulations 2017 and the Consumer Credit Act 1974 – along with relevant industry guidance and what I consider to be best practice at the time of the complaint.

I've read and considered all of Mr P's submissions regarding his complaint, and his detailed response to the provisional decision. But I'll concentrate on what I feel is relevant, which our rules allow us to do. If I don't comment on a specific point raised, this isn't because I've failed to take it on board or consider it appropriately, but because I don't need to comment on it to reach what I think is the right outcome.

I've noted Mr P's comments about my reference in the provisional decision to what a typical fraudster may do – which in this case meant there was no single specific pattern of behaviour I'd expect a fraudster to demonstrate in every single case.

However, in this case Mr P is alleging that he was the victim of a sophisticated fraud here – so at the very least I may expect the fraudsters to attempt to maximise the amount of money they can take in a short period of time. But here they instead had a working card and the PIN but made no attempt to use it for several weeks.

This would represent a tremendous risk that the address change would be discovered, and potentially the newly ordered card be cancelled by Mr P. We know he was accessing his online banking for the card after the address had been changed and could have noticed this change when he was checking the statements. And there was no attempt by a third party to gain access to, or control of, the online banking, despite having all the necessary information to do so.

Whoever had the card didn't feel rushed to make use of it – which is also reflected in the eventual usage over several days. So, I'm not persuaded that it was more likely that not the work of some unknown sophisticated fraudster. That there were no further attempts to use the card after it had been cancelled strongly suggest to me that whoever had the card was aware it would no longer work.

I've also not seen anything to suggest any other accounts Mr P held were targeted by fraudsters at the time – it seems confined to this one particular card, which seems unusual if an unknown third party fraudster had compromised his credit file.

I've reviewed the emails Mr P has provided between his employer at the time and him, which he says shows he couldn't have carried out the transactions. But I'm not persuaded this tells me anything other than Mr P had access to his emails at the time of the transactions. It also doesn't discount the possibility of a third party using the card with Mr P's consent – and we already know there was a third party involved by the voice on the phone.

I'm sorry if Mr P doesn't feel I've given appropriate weight to what he's provided. I have considered everything submitted to me. My decision doesn't hinge on a particular piece of evidence, or a single event, but rather by considering the totality of the evidence and placing appropriate weight on them. The only plausible explanation I can see is that the transactions were carried out either by Mr P or someone with his consent, for the reasons given above. Under the relevant sections of the Payment Services Regulations these would be authorised transactions and Sainsbury's can hold him liable for them, and it's not unreasonable that they ask for them to be repaid.

In regard to the marker recorded with CIFAS, I remain satisfied that the information held by Sainsbury's is enough to conclude that Mr P was involved in the transactions and would have known this at the time he reported them as fraudulent. On that basis, the standards of evidence required by CIFAS have been met, so I can't reasonably ask them to remove this marker.

My final decision

My final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr P to accept or reject my decision before 1 June 2023.

Thom Bennett
Ombudsman