DRN-3611802

The complaint

Mr K complains that Santander UK Plc won't refund transactions he says he did not make and does not recognise.

What happened

Mr K is disputing fourteen transactions that were debited from his Santander accounts.

At the end of October 2020, seven third party payments totalling £1,460 were initiated using Open Banking from Mr K's account ending 0981. Then in the days that followed, seven faster payments totalling just over £15,000 were made from Mr K's account ending 4718. Mr K has explained that he has no idea who the money has gone to or what that reference is in relation to.

Mr K has explained that he first discovered large amounts of money had been transferred between his accounts when he checked his online banking. He contacted Santander and raised a fraud claim about the faster payments from account ending 4718. He later discovered the Open Banking payments and added them to the claim, as well as reporting the matter to the police and Action Fraud.

Santander declined Mr K's fraud claim. It said it was unable to refund him because the transactions being disputed were authenticated using his mobile device via online banking.

In its final response, Santander maintained its position to decline the claim. It said it was unable to see how a third party could have accessed Mr K's online banking information or had access to the text messages that were sent to his registered mobile number when some of the disputed payments were made. Santander said that the device used to make the payments had been registered to Mr K's account and mobile number in July 2020.

Santander also paid Mr K £50 compensation in a separate final response to acknowledge the bank had caused him inconvenience by not telling him that his debit card had been restricted as it had potentially been compromised.

As Mr K was unhappy with Santander's position, he referred the complaint to this service. He said that the device used to make these payments wasn't his and he'd never owned that particular model of tablet. He provided details of his devices and their serial numbers along with details of his IP address. He explained that he'd never received any one-time passcode messages to his phone during the period that the money was taken.

Our Investigator asked Mr K to contact his mobile phone company. He did so and there was no evidence of anyone else accessing his mobile phone or swapping his sim. Our Investigator also asked Mr K questions about his phone and his payment tools. He said that no-one would have been able to access his card or his online banking details because he'd not shared them with anyone, nor did he think he'd inadvertently given them out by responding to any phishing messages. He explained that he'd always had a password on his phone and no-one else could have accessed it.

After making extensive enquiries, our Investigator was unable to see how anyone else would have been able to make the payments Mr K was complaining about. She didn't think it was likely that an opportunistic fraudster would have added the device to Mr K's account profile in July 2020 and then waited over three months to use it. She also couldn't see how anyone else could have obtained Mr K's new online banking log in details after he'd changed them in August 2020, nor could she understand how anyone else could have been in a position to positively respond to the one-time passcode messages sent to Mr K's registered phone number.

Mr K was disappointed with the outcome and asked for it to be reviewed. He explained that he'd not given his details to anyone. He said as much as there is no proof that he had not given details away or taken out the money, there was also no evidence to suggest that he did. He felt that it was his word against Santander's.

As no agreement could be reached, the complaint was referred to me for a decision.

My further investigation

As part of my review, I requested further information. When Mr K referred his complaint to us, he said he was going to ask Apple for a list of all of the devices his profile had ever been associated with. I asked Mr K if he had ever been able to obtain that information. He wasn't able to get that information directly from Apple, but he did provide screenshots of his Apple profile to show the devices he is currently connected with.

I also asked Mr K about a payment that I'd noted in the bank's technical records. It was attempted but abandoned without being made on 14 August 2020. It was set up using the tablet Mr K disputes owning. Mr K responded to say that he didn't remember the payment and suggested it may have been the fraudster trying to first access his account.

I noticed from the bank's records that the payments our Investigator had identified as card payments were actually Open Banking payments. I asked Santander when Mr K's profile had consented to use Open Banking. Santander responded to say the disputed third-party payments were the first time Mr K's profile had been used for any Open Banking activity. The bank highlighted the payment screens that would have been displayed at the time those payments were made.

I also contacted the third-party provider that had initiated the payments to find out more about what they were for, as this was not clear from Mr K's statements. The third-party provider responded and explained that it had offered a payment service on behalf of an online gaming company and it was the gaming company that ultimately received the funds. It explained that the gaming company's customer selects the third-party provider as the payment method, then the customer is redirected to an authentication screen provided by the customer's own bank to complete the payment. The third-party provider said the information it had obtained from the online gaming company about its customer matched Mr K's details.

I contacted Mr K and updated him on what I'd found out. I explained that to use a gaming merchant usually a potential customer needs to be verified with photographic ID alongside address verification so that the gaming company can meet its legal requirements. I asked Mr K if he recognised this company. Mr K said he'd never used online gaming services. He contacted the gaming company and discovered it held an account in his name. He provided evidence to show that the gaming company had now closed the account in light of his comments that it was opened fraudulently. The gaming company would not disclose any further information to Mr K about how and when the account was set up.

I noted that almost £650 of the disputed faster payments made from account ending 4718 had been recovered. I asked Santander if it knew more about why this money was returned. It provided what it could to me about the recipient's account in confidence.

I issued my provisional decision on 21 November 2022. In it, I explained why I didn't intend to uphold Mr K's complaint. An extract of that decision is set out below:

What I've provisionally 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.

When considering what is fair and reasonable, I am required to take into account: relevant law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to have been good industry practice at the relevant time. In cases when it is not clear what happened, I have to base my decision on the balance of probabilities. In other words, what I consider is most likely to have happened in the light of the available evidence. There's a lot of money involved in this dispute so I can understand why Mr K is concerned. But having considered everything that's been said and provided so far in this case, I can't see how the payments in dispute could have been made without Mr K's authorisation. This means that Santander can fairly hold him liable for the disputed transactions.

Whether a payment transaction has been authorised or not is important because the Payment Services Regulations 2017, which are the relevant regulations that apply to the payments in dispute, explain that account holders will usually be liable for payments they've authorised, and generally speaking, banks will be liable for unauthorised payments. If Mr K made the disputed transactions himself or agreed for them to be made on his behalf, it would not be fair to ask Santander to refund them. But Mr K says he was not involved in the payments in dispute.

I'm satisfied from the bank's technical records that personalised security information alongside payment tools issued to Mr K (such as one-time passcodes sent to his registered mobile phone number) were used to make the disputed transactions. But the regulations relevant to this case say that is not, on its own, enough to enable Santander to hold him liable. So, I also need to think about whether the evidence suggests that it's more likely than not that Mr K consented to the payments being made.

I've considered the options for what's most likely to have happened. These are that the transactions were made by an unknown third party, by someone known to Mr K either with or without his permission, or by Mr K himself.

Mr K has consistently maintained that he has no knowledge or connection to any of the payments that are in dispute. He's reported the matter to the police and to Action Fraud, and he's done as much as he can to try and find out how and when an account in his name was set up with an online gaming company. But these factors do not mean that the transactions are automatically unauthorised. I must consider the wider circumstances surrounding the payments in dispute.
I've thought carefully about how the payments in dispute were made. I have not gone into explicit detail about the bank's security processes, instead I have focused on the steps that someone making these payments would have needed to follow.

The bank's records show that the device that was used to make the payments in dispute was linked to Mr K's profile on 13 July 2020. To link the device to Mr K's credentials, a text message was sent to Mr K's registered mobile number. Santander has held the same mobile

phone number for Mr K since 2015 and it is the same phone number that Mr K has used when speaking to this service. Mr K has not suggested that there has been any problem with his mobile phone service or his handset at any point. He's confirmed there have been no problems with his phone service directly with his mobile phone company. He's also explained that no-one else would have been in a position to access his phone in order to intercept text messages without his knowledge or agreement. Against this backdrop, I can't see how an unknown third party could have registered the device without Mr K's knowledge.

The bank's records show that the device was used on 14 August 2020 to set up a payment that was not made. When I asked Mr K about this, he suggested that it could have been the fraudster first trying to access his account. It's not surprising that Mr K could not recall anything much about that specific day. Over two years had passed when I asked and ultimately, the payment was abandoned so no money left his account at this time. But if an unknown third party had been able to both link a device to Mr K's profile and then obtain his personalised online banking login details without him knowing, it seems unlikely they would not try to benefit as much as they could as quickly as they could. Mr K changed his online banking credentials on 26 August 2020 in response to an unconnected fraud, so even if an unknown third party had found out his personalised online banking login information to be able to log in on 14 August 2020, these credentials had been changed when the transactions currently in dispute were made. As a result, it seems unlikely that an opportunistic third party would have access to the details required to make these payments.

I've looked carefully at the process that is required to initiate an Open Banking payment with a third-party provider. We now know that the beneficiary of the funds that were sent as Open Banking faster payments was a gaming company and that the funds were deposited into an account in Mr K's name that matched his details. It's unclear how this account came to be. Mr K has explained that he's got no connection to it. I understand why Mr K is concerned about this. But it is not my role to establish the wider circumstances around how this account was set up. I am unable to determine how someone else could have got hold of Mr K's details or investigate who that person may be. My role cannot go any further than making a determination on whether Santander is entitled to hold him liable for the transactions that debited his Santander accounts.

The Open Banking faster payments were initiated within the gaming company's platform but authorised in Santander's platform. To log in to authorise the payments required Mr K's personal/customer ID, along with random characters from his personalised password and security number and recognition of a personalised image and phrase. Then, to approve payments, a one-time passcode was sent as a text message to Mr K's mobile phone number. I've thought about whether it would have been possible for these verification texts to have gone to another device without ever being seen on Mr K's phone. But there's no suggestion that Mr K had enabled any text messaging forwarding to other devices.

I've considered the possibility that someone known to Mr K was able to register a new device to his profile, potentially find out both his old and new online banking credentials, access his text messages either from his phone or by intercepting them and then go on to initiate these payments to a gaming account in Mr K's name and to another bank account. But Mr K has been clear that his phone has always been in his control. He's not shared his online banking details with anyone else and he's not allowed anyone to make transactions on his behalf at any point in the past. Against that backdrop, it is difficult to see how someone else would have had the opportunity to steal this much of Mr K's personalised security information.

I've looked carefully at the process required to make the faster payments that debited account ending 7418. The bank has provided evidence to show the transfers were made by someone logging in using Mr K's credentials. For the same reasons that I've already

outlined, I cannot see how someone else would have been able to log into Mr K's online banking and make these payments. The information Santander was able to provide to me about the receiving account did not provide any further insight into the wider circumstances.

I am sorry to have to deliver this news to Mr K. But from what I have seen so far, there is no explanation for how someone else would have been able to add a new device to Mr K's profile, obtain his up to date security credentials to be able to log into his online banking and also verify Open Banking transactions with one-time passcodes unless he'd allowed them to do so or been directly involved in making the payments. I realise that this is a very difficult message to give, but it is what the available evidence currently leads me to conclude. This means that Mr K is considered to have authorised the transactions in dispute and Santander has not acted unfairly by holding him responsible for them.

Responses to my provisional decision

Santander responded to say it had received the provisional decision and had nothing further to add.

Mr K responded to say he was extremely disappointed with the proposed outcome. He made six key points, which I have summarised below:

- Even though the investigation cannot prove anyone else had been able to make payments, that does not prove that he made or authorised them
- Santander did not explain why it had returned almost £650 to him. He suggested that for the bank to return any money at all, it must be admitting it was liable for the money being taken
- He would not have contacted the Police and Action Fraud if he was involved in making the transactions
- He regularly receives phone calls from fraudsters pretending to be Santander and the callers know his account number and sort code, so someone has some of his banking details
- He did not make the fraudulent payments and Santander cannot prove that the payments were taken with his consent
- He has no reason to commit this fraud. He holds a respected job and holds his mortgage with Santander, so there is no motive for him to commit fraud against a bank so intrinsically linked with his life

Mr K asked me to reconsider my view and said this is a case of bank and identity fraud.

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've reached the same conclusion as I did in my provisional decision, which is set out above and forms part of this final decision. I have done so even after taking into account Mr K's comments. I'll explain why.

This is not a decision that I have reached lightly. I'm aware that this money was Mr K's savings and I can understand why he feels strongly about what has happened here. He's maintained from the outset that he never authorised or agreed that anyone else could make the disputed payments.

But it is not my role to find out who actually made these transactions. The key issue I have to determine is whether Mr K can be held responsible for them. Having looked carefully at all of

the circumstances surrounding the disputed payments, I can't fairly say that Santander should bear the loss.

Mr K has pointed out that some of his banking details must be in the hands of fraudsters because of the number of scam calls he receives. But to make these transactions required more than the knowledge of Mr K's sort code and account number.

It remains the case that I cannot see how anyone else could have registered the disputed device or known Mr K's personalised security credentials to be able to log into his online banking, especially since the disputed transactions were made after he'd changed those details. In addition, I still cannot see any plausible way for someone to have intercepted the one-time passcodes sent to Mr K's registered mobile number and used to verify some of the payments in dispute.

Mr K has pointed out that Santander returned almost £650 to him and asked why the bank did not return more. I can see why Mr K thinks that returning any money at all must be linked to the decision of liability. But this amount is what remained of the disputed money that was sent from Mr K's account ending 4718. I am unable to specifically comment on the account that received Mr K's money as it belongs to a third party. I have investigated the wider circumstances around the recovery of these funds to see if they shed any more light on the issues at hand here, but they did not.

I am sorry to have to disappoint Mr K. But I am still not persuaded that it would be unfair for Santander to hold him responsible for the transactions. From the evidence I have, I can only conclude that Mr K made the transactions or gave someone else permission to make them.

My final decision

For the reasons I've given, my final decision is not to uphold Mr K's complaint against Santander UK Plc.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr K to accept or reject my decision before 4 January 2023.

Claire Marsh
Ombudsman