DRN-5308794

The complaint

Miss M complained because Kroo Bank Ltd refused to refund her for transactions which she said she hadn't authorised.

What happened

On 22 February 2024, there were multiple debits to Miss M's account. These were to two organisations in different countries abroad, and totalled £4,560.65.

The same day, Miss M contacted Kroo by chat, and said she didn't recognise the payments. Kroo asked Miss M a number of questions, including whether anyone else had access to her card or app, where she recorded her PIN, and whether she still had her card. Miss M replied that no-one else had access to her card or app, and her PIN was only recorded on her Kroo app. She said she'd never used the merchants before and didn't know what the companies were. She said no-one had asked to use her account, and her phone hadn't been out of her possession. Nor had she received any unusual calls, and she said she didn't answer calls from numbers she didn't recognise anyway.

Kroo asked more questions over the next fortnight, including whether Miss M had received any odd phone calls claiming to be from any organisation. Miss M said she hadn't, and there had been nothing unusual with her phone or email. Nor had she had any suspect messages about a missed delivery. Kroo asked whether she'd received any codes to her email or phone around 20th. Miss M said no. Kroo then told Miss M it had sent her a One Time Passcode (OTP) to her phone at 10.08 am on 20 February, and asked her if she could view this. Miss M said she didn't recall receiving a code that day, and if she had, she'd have deleted it if she didn't recognise it.

On 5 April, Kroo told Miss M that it had investigated and wouldn't refund her. It said this was based on multiple factors, including the information she'd given, review of the transactions, and evidence from internal systems and regulations.

Miss M complained.

On 7 May, Kroo sent its final response to Miss M's complaint. It said that Miss M had said she was the sole user of her Kroo card and app, and that her phone hadn't been out of her possession. And it had also asked her other questions, including details of any unusual activity or communications she might have received. Kroo said that it had reached its outcome using a combination of the information Miss M had provided, and the data it held about the transactions. It said that evidence supported its view that the disputed transactions weren't fraudulent, so it wouldn't refund her.

Miss M wasn't satisfied and contacted this service.

Miss M told us that she didn't know who the companies were, and hadn't authorised any payments to them. She said no-one else had access to her card and PIN, and had reported it to Action Fraud. Miss M said that she'd used her Kroo account for savings, so her back-up

money had now gone. Also, part of the money had been inheritance from a family member, which made it more upsetting.

Our investigator didn't uphold Miss M's complaint. She explained that Kroo had sent evidence showing that the payments had been authenticated from a device where her card was registered using a mobile payment service. As Miss M still had the device, and she'd said she hadn't shared any of the security details, the transactions couldn't be considered unauthorised.

The investigator also explained that Kroo had provided evidence to show that a OTP had been sent to the mobile phone number which it held on file for Miss M – and that was the same number which Miss M had given this service as her contact number.

So the investigator said there was no reasonable explanation for how anyone could have known the details of the OTP, and gained access to Miss M's phone, when the phone had been in her possession throughout.

Miss M didn't agree.

She asked how Kroo had advised that a mobile payment service had been used, as she said she'd never used this. She said she might have received a code, but nothing to say what it was for, and nothing about any transactions needing to be authorised or due to go out. She said she most definitely wouldn't have authorised this amount to go to companies abroad she knew nothing about.

Miss M looked up the mobile payment service, and said she'd read that this was a common way to scam, with the scammers buying vouchers online, then claiming or selling them anywhere in the world. She said this must have been what happened with the companies abroad.

Miss M also said that her money should have been protected by the Financial Services Compensation Scheme. She also said she wasn't happy that Kroo hadn't refunded the money, which had been sent to two random companies abroad through the mobile payment service, without her consent.

Miss M asked for an ombudsman's decision.

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.

There are regulations which govern disputed transactions. The relevant regulations here are the Payment Services Regulations 2017. In general terms, the bank is liable if the customer didn't authorise the payments, and the customer is liable if they did authorise them. I understand that losing savings, especially when part of an inheritance, would be very upsetting. But what I have to look at is whether it's more likely than not that Miss M, or a third party fraudster unknown to her, carried out the disputed transactions.

What helps decide this is the technical computer evidence about what happened on Miss M's account at and around the time of the disputed transactions. This shows that at 10.08am on 20 February 2024, a new mobile payment token was registered to Miss M's account. I've seen the computer evidence which shows that in order to set this up, a text was sent to the phone number which was registered to Miss M's Kroo account. That phone number is the same one which Miss M gave this service as her contact number.

The text said: ‘’*Your activation code is* [a 6 digit number] *for adding your Kroo card to* [name of mobile payment service]. *This code expires in 30 min. We will never ask you to share this code.’’*

The code was correctly entered which resulted in the new mobile payment token being approved. There are 1,000,000 possible combinations of any 6-digit number, so no-one could have guessed the code. So whoever approved this token must have had access to Miss M's mobile phone. One this token had been set up, the disputed payments were made using the token.

But Miss M said that she had her phone throughout, and that no-one else had access to it. So I can't see how it could have been a third party fraudster unknown to her, or even anyone close to her with access to her phone, who set up the token which enabled the disputed payments to take place.

Sometimes, a scammer will try to obtain a code from a consumer, such as the OTP which Kroo sent to Miss M's registered phone number and which was used to authorise the token. If a consumer gives someone that code, the fraudster could then make fraudulent payments. Or the customer can be tricked into making payments themselves at the scammer's instruction. Different rules apply when this happens, but that isn't what Miss M said happened here. She told Kroo that she hadn't had any unusual phone calls or emails, and that although she didn't remember receiving a code on 20 February, if she had, she'd just have deleted it. So whatever happened here, it wasn't that Miss M had been tricked into giving a scammer the necessary code to set up the token which enabled the disputed payments to be made.

The mobile payment token which enabled the disputed payments to be made was set up by someone correctly entering a code which had been sent to Miss M's registered phone. And Miss M's evidence is that the phone was in her possession throughout, and no-one else had access to her phone or details. Miss M also didn't say she'd been tricked into giving out the code to a third party.

All this means that I can't see any way that a third party fraudster could have set up the token which enabled the disputed payments. Logically, it must have been set up by someone with access to that phone and to the OTP sent on 20 February. So I can't find that it was a fraudster who carried out the disputed payments, and I can't uphold this complaint.

Finally, Miss M said that her money should have been protected by the Financial Services Compensation Scheme (FSCS). The FSCS helps consumers when a financial business is unable – or likely to be unable – to pay compensation due from a claim against the business. This usually happens when a business is insolvent or has stopped trading and doesn't have enough assets to pay claims made against it. That's not the situation here.

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 Miss M to accept or reject my decision before 7 March 2025.

Belinda Knight
Ombudsman