

The complaint

Mr C is complaining that Kroo Bank Ltd hasn't refunded transactions which he says he didn't authorise.

What happened

Around 5.30pm on 12 June 2024 Mr C received a call from a mobile number. The caller (who I'll refer to as the scammer) said they were from Kroo and they were calling because there were some suspicious transactions on Mr C's account.

Mr C says the scammer knew many of his personal details including his full name, and the last four digits of his card number. Mr C has stressed the pressure and urgency of the conversation, with the scammer impressing upon him that he needed to act quickly to secure his account. The scammer said that as part of the security procedure a security code would be sent to Mr C's device. Mr C said two codes arrived by text message and he was asked to read them out to the scammer. The scammer reassured Mr C that he was working in the background to secure the account and the call ended.

After the call Mr C reflected and felt unsettled about what had happened, so he logged into his Kroo account. He found that multiple transactions had been made on his account and were continuing to happen. He tried to freeze his account and card through the app but wasn't immediately able to find the option to do so. He says he looked for a phone number to call Kroo but could only locate a number which operated until 5pm. He did manage to freeze his account and card, but only after 18 transactions totalling £9,078.35 had been made. The transactions were made to what appears to be a shop located abroad, a money transfer service and a gambling company.

Mr C complained to Kroo about what had happened. But Kroo didn't uphold his complaint. It said that Mr C's security credentials were shared which allowed Apple Pay and Google Pay tokens to be bound to his Kroo debit card, which is how the disputed payments were made. It concluded Mr C had been grossly negligent in sharing the security credentials and therefore it wasn't liable to refund the payments.

Our Investigator asked Kroo for some more information, including the terms and conditions applicable to Mr C's account at the time, evidence to show how Apple Pay and Google Pay were set up on the device(s) used to make the payments including how the activation codes were used to do so, and full details of the individual transactions to show how and where they were carried out and how they'd been authenticated.

Kroo didn't send this information to the Investigator, so she reached her view of Mr C's complaint based on the evidence she had. She said, in summary:

- She hadn't seen evidence to show exactly how Apple Pay and Google Pay were set up or how the payments had been carried out. But looking at what she did have, while she accepted that although Mr C had likely shared the activation codes with the scammer, he didn't understand that sharing this information would result in payments debiting his account. He thought he was speaking to a genuine Kroo representative and was

securing his account. So, she didn't consider he'd consented to the payments and could only reasonably conclude that the payments were unauthorised under the PSRs.

- While she accepted Mr C likely shared codes with the caller, she hadn't seen evidence that the codes were used, or how they were used, to set up Apple Pay and Google Pay, nor that the disputed transactions had been carried out using them. So, she couldn't fairly say that Mr C had failed with gross negligence.
- As a result of her findings, she thought that Kroo should refund all the disputed transactions, with 8% interest.

Kroo didn't respond to the Investigator's view within the time she specified, although Mr C accepted it. But Kroo provided some more information, including about how Apple Pay and Google Pay were set up in order to make the disputed payments.

Mr C's complaint was passed to me for review and a decision. I issued a provisional decision on 18 November 2025. This is what I said.

"Did Mr C authorise the payments?"

I've firstly considered whether Mr C authorised these payments. This is relevant as, in line with the Payment Services Regulations 2017 (PSRs), he would generally be liable for payments he authorised – whereas Kroo would be liable for unauthorised payments. The PSRs say that Kroo, as the payment service provider, is responsible for demonstrating that a payment transaction has been authenticated and executed correctly.

The PSRs specify that authorisation depends on whether the payment transactions were authenticated correctly – and whether Mr C consented to them. It's not disputed the payments were authenticated correctly (as in, the correct payment steps were completed). So, I've gone on to consider whether Mr C consented to them.

The PSRs specify how consent is given – it must be in the form, and in accordance with the procedure, agreed between Mr C and Kroo. Kroo has now given us the terms and conditions that applied at the time the payments were made. But they don't set out in detail how Mr C consents to making payments using Apple Pay and Google Pay, which is the nature of the payments in dispute here. So, I've looked at the practical steps that would've been needed to make the payments. It seems Mr C would have needed to use his device and its associated biometrics with the merchant to make them.

It's not clear how the scammer obtained Mr C's card details – Mr C hasn't mentioned sharing his card details with the scammer and says the scammer was initially able to give him the last four digits of his card number which convinced him they were genuine. But it doesn't appear to be in dispute that the scammer set up Apple Pay and Google Pay on their own device(s) using Mr C's card details and made the payments. It follows Mr C hasn't used the agreed form and procedure to consent to these payments.

Kroo has now given us some more information about how Apple Pay and Google Pay were set up on the scammer's device(s). It's told us that the tokens were not set up within Kroo's app – instead, Mr C's card details were entered into the relevant Apple Wallet or Google Wallet app on the scammers device(s). Activation codes were then sent to Mr C by text message, and it seems these were entered into the device(s) by the scammer in order to set up the tokens. Kroo has argued that Mr C shared the activation codes with the scammer which allowed this to happen.

It does seem that the scammer tricked Mr C into enabling them to set up Apple Pay and

Google Pay under the guise of keeping his account safe. But based on what Kroo's now told us, it doesn't appear that Mr C did anything himself to authorise either the creation of the new payment tokens or the payments themselves.

While it does seem that Mr C shared the activation codes to set up Apple Pay and Google Pay, he did so on the understanding he was keeping his account safe. I don't think he understood he was, in fact, allowing someone to set up Apple Pay and Google Pay with the intention of making payments from his account, or that he did anything himself to give Kroo the impression that he'd given permission for anyone to make the payments on his behalf.

Considering that Mr C was tricked into allowing someone to set up Apple Pay and Google Pay, I don't think it would be fair to say he gave a third-party permission to consent to payments on his behalf. It follows that I'm satisfied the disputed payments were unauthorised. This means the starting position under the PSRs is that Kroo is liable to refund them.

Did Mr C fail with gross negligence?

Kroo submits that even if these payments are to be considered as unauthorised, it shouldn't be held for liable them. That's because it thinks Mr C failed with gross negligence to keep his personalised security details safe – something which, if proven, would mean he wouldn't be entitled to a refund under the PSRs.

From the new information Kroo has supplied, it seems Mr C shared the activation codes with the scammer during the phone call which were then used to set up Apple Pay and Google Pay. Kroo says that from the text messages Mr C received it would have been clear what the codes were for, and they included a warning not to share them.

I've reflected on the circumstances that led to the scammer gaining access to the activation codes. I appreciate that the text messages do mention that the codes are Apple Pay and Google Pay activation codes. But in the circumstances here, where Mr C believed he was speaking to a representative of Kroo, I can understand why Mr C would have thought he was keeping his account safe when he shared them.

The text messages do include a warning not to share the codes but I don't think Mr C would have thought that would apply to sharing them with someone who, as he thought, worked for Kroo. And I'm also taking into account that at the time Mr C was being put under a lot of pressure to act quickly to protect his account.

This isn't to say Mr C acted perfectly reasonably here. But having considered the circumstances carefully, I'm unable to reasonably conclude that Mr C's loss was caused by him failing with gross negligence.

Kroo has now mentioned what it considers to be a similar case where the Investigator's view was that Kroo and its customer should share liability equally, and it's said it feels this would be a fairer outcome in Mr C's case. I must decide Mr C's case on its own merits - but it may be helpful to explain that in the case Kroo has mentioned I can see that the Investigator found the payments were authorised.

In this case, I have found that the payments were not authorised and that Mr C hasn't failed with gross negligence. It follows that, in line with the PSRs, I don't consider Mr C can be fairly held liable for these unauthorised payments and Kroo must put things right – by refunding his losses from the payments alongside 8% simple interest per year to compensate him for the time he's been out of pocket.

For the reasons I've explained, my provisional decision is that I uphold Mr C's complaint. Kroo Bank Ltd must:

- *Pay Mr C the total of the unauthorised payments, less any amount recovered or refunded.*
- *Pay 8% simple interest per year on this amount, from the date of the unauthorised payments to the date of settlement (less any tax lawfully deductible)."*

Mr C replied to say he accepted my provisional decision.

Kroo replied to say it had nothing else to add.

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.

As Mr C accepted my provisional decision, and Kroo had nothing else to add, I see no reason to depart from it.

My final decision

My final decision is that I uphold Mr C's complaint. Kroo Bank Ltd must:

- Pay Mr C the total of the unauthorised payments, less any amount recovered or refunded.
- Pay 8% simple interest per year on this amount, from the date of the unauthorised payments to the date of settlement (less any tax lawfully deductible).

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr C to accept or reject my decision before 18 December 2025.

Helen Sutcliffe
Ombudsman