DRN-3871555

The complaint

Miss K, in her capacity as the director of a limited company "K", complains that Revolut Ltd won't refund transactions she didn't authorise.

What happened

The full details of this complaint are well known to the parties, so I won't repeat them again here. Instead, I'll recap the key points and focus on giving my reasons for my decision:

- In August 2022, Miss K received a call from someone purporting to be from Revolut. The individual told her that someone had attempted to make a payment using Apple Pay and her business account needed to be secured. Miss K states that the caller already had a lot of information. Under the guise of safeguarding the account, Miss K followed the caller's instructions and shared the information that was requested.

- The fraudsters made payments totalling just over £28,000 from K's Revolut account. Majority of the transactions were made in-store through Apple Pay and two were processed online. Later that day, Miss K saw emails from Revolut about declined transactions and realised that money had been fraudulently taken from K's account. She immediately reported this to Revolut. It said it was unable to present a chargeback as all the disputed transactions had been processed using an authorised device. Revolut declined to reimburse the money as it believed Miss K was liable for the loss, given that she allowed third-party access to the account by sharing information.

- The matter was referred to our service and our investigator didn't agree with Revolut that K should be held liable. They recommended it to refund all the transactions along with interest and pay £100 compensation. Revolut disagreed and so the complaint was passed to me to decide.

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 agree with the conclusions reached by the investigator for the following reasons:

- The starting point for any complaint about unauthorised transactions is the Payment Services Regulations 2017 (PSRs). Broadly speaking, K is responsible for any payments Miss K – acting on its behalf – has authorised (either by making them herself or allowing someone else to). And K isn't liable for payments it didn't authorise, unless Miss K failed with intent or gross negligence to comply with the terms of the account or keep the account security details safe.

- The investigator's view was that the payments were unauthorised. I can't see that Revolut has explicitly disagreed with this finding; its response to the view has

focused on negligence on Miss K's part in keeping the account credentials safe. Nonetheless, I've first thought about whether the payments were authorised. For a payment to be authorised, Revolut must show that it was authenticated correctly and why it thinks Miss K consented to it.

- I've looked at Revolut's business account terms and conditions, and they don't specify the precise form and procedure for making an Apple Pay or online payment. The likely steps needed for an Apple Pay payment were presenting the Apple Pay enabled device and using FaceID/TouchID/passcode to confirm. And for the online payments, the likely steps were entering the card information, selecting pay, and if prompted to 3DSecure – confirming those payments within the banking app. It's unclear from the available information whether in-app verification was requested for either of the online payments.

- The payments may have been authenticated correctly but having considered the available information, I'm not persuaded that Miss K consented to them or to someone else making them on her behalf. Firstly, she states that her mobile phone works on the Android operating system and she doesn't own an iPhone. I'm not aware that it is possible to set up Apple Pay on an Android device. Secondly, her actions were that of someone who was intending to *protect* their money from fraud. Not consenting to someone else making payments on their behalf. I'll explain why.

- Miss K received a call from someone impersonating Revolut. The caller created a sense of panic and Miss K says that she did notice an attempt to use her card when she checked the mobile app. The scammer purported to be from her trusted bank and was already aware of this attempt. And, according to Miss K, they already knew information about her and the account. Miss K genuinely believed that she'd been contacted by Revolut and that it was taking steps to safeguard her money.

- As Miss K was then satisfied that she was communicating with her bank, I can't fairly say that it was unreasonable that she complied with the caller's request to provide the verification code to secure the account. I think that many people would have followed the instructions and complied with what they were being asked. Especially in the context of (in their mind) protecting their money from fraudsters. Indeed, we've seen many others who've acted in the same way that Miss K did.

- Revolut has said that Miss K also provided her card details. We've asked her about this, and she only remembers being asked to share the verification code. Miss K's been consistent in her testimony to Revolut and this service that the caller quoted the last four digits of the card in question to her. It's unclear how they already had this information, but I'm persuaded more by what Miss K has said all along. Namely, that she only gave out the verification code during the call.

- Revolut says it is obvious that the verification code is for verifying Apple Pay and not for deactivating Apple Pay as Miss K says the caller told her. I don't think it is that obvious. The text message reads, *"Revolut verification code for Apple Pay…"*. I don't think this makes it clear enough that the code is for activation or setting up of Apple Pay. It can also be read as verification that a request or instruction has been received in relation to Apple Pay (regardless of whether that request is to install, uninstall, or approve a payment using that method).

- I've seen the warning in Revolut's text message containing the verification code that says to never share it with anyone. But it looks like Miss K was acting quickly, so I can see how she may have missed this and focused more on the instructions she

was given from someone who she thought was trying to help. I don't think Miss K's actions in that moment mean that she *seriously* disregarded an *obvious* risk. I don't think her actions fell so far below what a reasonable person would have done in the same circumstances such that I think they amount to gross negligence – the test that's relevant here.

- Overall, I find that K isn't liable for the transactions in dispute. This is because they weren't authorised by Miss K and she didn't fail with intent or gross negligence to keep the security details safe. Revolut ought to have refunded the transactions much sooner. Miss K has told us that the cashflow problems have financially strained K's operations. She's also told us about how this situation has impacted her personally. Given that the transactions were made from a business account, I'm only limited to considering the impact on Miss K's business and not her personally. Having given this a lot of thought, I consider the amount of £100 that the investigator recommended in their view fairly recognised the inconvenience K has been put through because of this delay.

Putting things right

To put matters right for K, Revolut Ltd needs to:

- Refund all the disputed transactions;

- Pay 8% simple interest on this amount, from the date of the unauthorised transactions to the date of settlement (less any tax lawfully deductible); and

- Pay K £100 compensation.

My final decision

For the reasons given, my final decision is that I uphold this complaint. I require Revolut Ltd to put things right as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss K – on behalf of K – to accept or reject my decision before 9 February 2023.

Gagandeep Singh
Ombudsman