DRN-3317236

The complaint

Mrs L complains that Cynergy Bank Limited ("Cynergy") have unfairly refused to refund over £11,000 she lost as part of a scam where she was tricked into sharing her security details to a scammer pretending to be from Sky.

The details of this complaint are well known to both parties and have also been set out extensively by the investigator, so I will not repeat everything again here. Instead, I will focus on giving the reason for my 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.

Having done so, I agree with the conclusions reached by the investigator and have decided to uphold it. I'll explain why.

Cynergy submit that Mrs L authorised the payments that were made from her account on 5 January 2021. But in order for a payment to be regarded as 'authorised' under the Payment Services Regulations 2017 ("PSRs 2017") it is necessary for Mrs L to have given her *consent* to the execution of the relevant payment transactions. And, according to Regulation 67 of the PSRs 2017, consent *"must be given in the form, and in accordance with the procedure, agreed between the payer and its payment service provider*".

However, in this instance, I'm not persuaded that Mrs L did complete all the necessary steps in order to give her consent for a transaction to be made *"in the form, and in accordance with the procedure agreed".* I appreciate that she took the initial step of logging on to her internet banking, and also scanned her security device in order to authenticate the payments. But Mrs L was duped into doing this by being told that she had to 'approve' the transaction in order to receive a refund. She did not enter any payee details into her internet banking, for example, and was unaware that she was authenticating a payment to be made from her account. So, I'm not persuaded she can be said to have given her *consent* to the execution of the payment transactions, as she was under the impression that money would be paid into her account, not being transferred out of it.

The payment services directive itself (which the PSRs 2017 implement) states that *"in the absence of such consent, a payment transaction shall be considered to be unauthorised*". Therefore, given I don't consider Mrs L provided her consent for these payments to be made from her account, I'm satisfied they are to be considered as 'unauthorised' for the purposes of the PSRs 2017.

Did Mrs L act with intent or gross negligence – particularly taking into account the terms and conditions of her relationship with Cynergy and the obligations set out in the PSRs 2017?

I don't think Cynergy have suggested that Mrs L failed to comply with her obligations under Regulation 72 of the PSRs with *intent,* and neither have I seen any evidence that would

suggest this either. So, I do not intend to explore this point any further as I don't consider she failed to meet her obligations with intent.

However, I have considered whether the actions Mrs L took fell so far below the standard of a reasonable person that she could be said to have failed with gross negligence to take all reasonable steps to keep her security information safe or to comply with the terms and conditions of her account.

Gross negligence is not an abstract concept. It's important to take into account all the circumstances when considering whether an individual's actions amount to gross negligence. Scams such as the one experienced by Mrs L are very sophisticated, and it's likely the fraudster used a range of social engineering techniques to trick, deceive and manipulate her into following their instructions and inadvertently allowing access to her internet banking.

Mrs L has explained that Sky is her broadband provider. She has also said that she had been experiencing issues with her connection, So, when the scammer contacted her purporting to be a Sky engineer that wanted to test her connection speed, she wouldn't have immediately thought there was any reason to doubt the legitimacy of the person she was speaking to.

When discussing the refund Mrs L was due, the scammer also knew the last four digits of her bank account number, which would've further persuaded her that it was a legitimate call from her broadband company. She was also passed between different people/departments and even spoke to a 'manager' to give the appearance of a legitimate operation.

When Mrs L downloaded the remote access software, the fraudster managed to convince her that they could not see her internet banking screen, and she was reassured that it was only required so their server could connect to her bank to authorise the payment. They managed to black out her screen and also used convincing looking logos of Sky while they ran 'tests', and continued to be reassure her that they could not see her screen, at which point she agreed to log on to her internet banking to see if the refund had been received.

I don't think it's entirely implausible for Mrs L to think that she might be due a refund if she had been experiencing connection issues as she had. And she said the scammer always had convincing and plausible answers to any of her questions when she had doubts. It was all of these circumstances combined that led Mrs L to ultimately trust the person she was speaking to, and to follow their instructions to download the remote access software and follow the Cynergy payment authentication process (albeit for a refund to be issued rather than making any payments).

I appreciate that Mrs L undertook the authentication process several times, as the scammer told her this was necessary. But she has explained that she was in a rush and wasn't thinking straight as she had to attend to her children's home schooling, and she had already been on the phone for a significant amount of time. She was under pressure to get it sorted as soon as possible, and given she thought she was dealing with a business she knew, trusted and had dealt with before, I think a lot of people would have done the same thing and believed what the scammer was saying.

On balance, I'm satisfied that Mrs L thought that by downloading the remote access software and following the authentication process that she was enabling a refund to be paid into her account. It was in this context that she took the steps that she did, and I think a lot of people in a similar position would've behaved in a similar way in those circumstances. It therefore follows that I don't think the actions Mrs L took fell so far below the standards of a reasonable person, such that she could be said to have failed with gross negligence to keep

her personalised security details safe or to comply with the terms and conditions of her account. And so I conclude that it would be fair and reasonable for Cynergy to provide a full refund to Mrs L's account of the amount that she lost.

My final decision

For the reasons given above, I uphold this complaint and direct Cynergy Bank Limited to refund Mrs L the money she lost as part of the scam, less any amounts subsequently recovered. Cynergy should also pay 8% simple interest per annum on this amount from the date of loss until the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs L to accept or reject my decision before 6 September 2022.

Jack Ferris
Ombudsman