DRN-4590753

The complaint

Miss L complains that National Westminster Bank Plc (NatWest) is holding her liable for payments she says she didn't make.

What happened

Miss says a number of unauthorised payments were taken from her NatWest account in early 2022. These were mainly sent to a recipient I'll refer to as O. But it appears she is also disputing two payments showing as sent to an account in her own name, which I understand were sent to a cryptocurrency account.

When contacting NatWest initially, Miss L said she didn't know anything about the payments. She mentioned someone else possibly having access to her account, but said she didn't think they had made these payments. NatWest asked Miss L about one of the cryptocurrency payments she is now disputing – and she confirmed she had made it. When NatWest told her it had been made using the same device used to make the disputed payments, she seemingly opted not to pursue a dispute.

Several months later, Miss L complained to NatWest via a professional representative about its refusal to refund her for the payments. She said the payments were linked to a cryptocurrency scam she fell victim to. She said she had got to know someone who was meant to be helping her with cryptocurrency investing. He sent her a link and she had to fill in certain details, which she thinks allowed him to access the account and make these payments without her permission.

NatWest didn't uphold Miss L's complaint about its refusal to refund her. She referred her complaint to our service. Our investigator also didn't uphold it. In summary, they thought there were inconsistencies and changes in Miss L's explanation of what happened. They thought she had probably granted access to her account. They thought it was unclear if this was due to a scam – but even if it was, they didn't think there were grounds to hold NatWest liable for the resultant loss.

Miss L has appealed the investigator's outcome. She says the payments weren't authorised as she was tricked into granting access to her account. And the phone used to make the payments isn't/wasn't hers. I've since been in touch to set out my understanding of what happened, to give Miss L a chance to comment. She hasn't responded by the (extended) deadline I set. So, I'm now proceeding to issue my final 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've decided not to uphold it. I'll explain why.

Broadly, the starting position under the Payment Services Regulations 2017 (PSRs) is that Miss L would be liable for payments she authorises. But NatWest would generally be liable for unauthorised payments taken from her account.

The PSRs make it clear that a payment is authorised if Miss L consented to the execution of it. And that consent must be given in the form, and in accordance with the procedure, agreed between her and NatWest.

In practice, that means a payment is authorised if Miss L completes agreed steps to make a payment (such as accessing the app, setting up a payee, and selecting an amount to send to them). But it's also authorised if she gave someone access to use that agreed form and procedure to make a payment.

I know Miss L says she was tricked into entering details via a link, which O then used to access her account without her consent. But her explanation over time has shifted. I place most weight on what she told NatWest in March 2022, when first disputing some of these payments – as that is when her recall will have been most reliable.

At that time, Miss L's response suggested she had given someone else access to her account – albeit she didn't think that individual had made the payments. She also confirmed making one of the payments she is now disputing. This contradicts what she has since told us – that she didn't make any of the payments, and that she didn't grant someone else access to her account.

I'd also point out Miss L seems to suggest O got access to her account through her entering her card details on a website link. But the card details wouldn't be sufficient to get access to authorise these transfers via mobile banking.

NatWest isn't the only account provider with whom Miss L has disputed payments, seemingly also alleging O to be the perpetrator. Looking at what Miss L has said, it's unclear to me whether the link she has mentioned related to her NatWest account, or another account.

I have also seen an exchange between Miss L and (who I understand to be) O, around six months after the NatWest payments were taken, in which she appears to be aware they have access to – and are making payments from – another account. I struggle to reconcile that with Miss L's assertion she didn't knowingly grant access to her NatWest account. If that was the case, it seems unlikely she would go on to grant further access to O.

Overall, I've concluded Miss L likely allowed O to act as her 'agent' – as in she permitted them to use her account to make payments. While she may not have been aware of each and every payment made, they would still be treated as authorised under the PSRs due to the access/authority Miss L effectively granted. Meaning she is presumed liable for the payments in the first instance.

I have considered if there are other reasons why NatWest holds any liability for the loss Miss L is alleging. As I've found these payments were authorised, and there is an allegation they were made as a result of a scam, I have considered whether NatWest holds liability under the CRM code. When the criteria of the code are met, victims of authorised push payment (APP) scams should generally be reimbursed – unless the account provider can show an exception applies.

The payments to Miss L's own cryptocurrency account aren't covered. As the CRM code doesn't cover me-to-me payments – nor does it cover payments to accounts that aren't held in pounds sterling (such as cryptocurrency wallets). For those payments sent to O, there is a suggestion from her that these were sent on to her cryptocurrency account. So, on the evidence provided, it's not clear whether these are covered.

But even if they are – which would also mean accepting the situation was an APP scam, which would require accepting Miss L made (or gave some access to make) the payments for what she believed were legitimate purposes but which were in fact fraudulent – I'm not persuaded NatWest can fairly be expected to refund her.

That's because one of the exceptions under the code is when the customer doesn't have a reasonable basis for believing the person she was dealing with was acting legitimately/that the services she was seeking were legitimate. There are a few reasons why I think this applies.

I can't see how Miss L could have thought it was above board that she needed to grant someone else access to her account – as she told NatWest in March 2022. Nor has she provided sufficient evidence of her contact with the individual from that time, or of her cryptocurrency account, to show how/whether she thought this was all part of a legitimate investment.

Miss L has suggested her contact with O primarily happened on a messaging app, where the messages are only available for a short period of time, as a reason why she can't provide further contact records. I think most people would realise an investment being advertised in this way, which required you to grant account access, probably wasn't legitimate.

I also don't think we have an adequate explanation for why Miss L said she had no knowledge of the payments at all in March 2022, but then submitted they were connected to a cryptocurrency scam when she complained via a representative. Similarly, it's unclear why she opted not to pursue a dispute with the bank at that point if she had been tricked into making the payments (or tricked into granting someone else access to her account).

I therefore think NatWest isn't obliged to refund these payments under the CRM code, due to the exception that applies even if the other qualifying criteria are met. I'm also satisfied NatWest met its obligations under the code, and its broader fraud-prevention expectations. None of the payments looked unusual enough, in amongst Miss L's normal activity, that I consider it remiss not to have intervened or issued warnings at the time the payments were made. In any event, any warnings would have been seen by the person who had access to her account rather than Miss L, so probably wouldn't have prevented the payments.

I appreciate this will be disappointing for Miss L. But, having carefully considered all the circumstances, I'm not persuaded it would be fair to direct NatWest to refund her for the loss.

My final decision

For the reasons given above, 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 L to accept or reject my decision before 12 March 2024.

Rachel Loughlin
Ombudsman