DRN-4801238

The complaint

Mr F complains that National Westminster Bank Plc ('NatWest') hasn't refunded payments made from his account to an investment scam.

What happened

This case involves five payments made in October 2023. Initially Mr F said he didn't make any of these. Then when NatWest pressed him on the matter and getting the Police involved, Mr F changed his testimony.

Mr F said he received a cold call from a company offering him an investment opportunity. He made a payment of £120 and expected to receive returns of £1,000 from this. Mr F then says he went to bed and the following morning saw that four other payments had been made to the same destination, but without his consent or knowledge.

NatWest explained the payments were all made via Open Banking, so started elsewhere, but were then approved in Mr F's app on his device. So it determined all the payments were authorised. It didn't agree to reimburse Mr F the funds under the Contingent Reimbursement Model code ("CRM code") and so declined his claim. Mr F disagreed with this outcome and brought his case to our service, but our Investigator also didn't uphold the case. Mr F asked for an ombudsman to review his case and maintained he only authorised the first payment.

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.

The starting position in line with the Payment Services Regulations 2017 ("PSRs"), the relevant legislation here, is that Mr F is liable for payments he's authorised, and NatWest is liable for unauthorised payments.

For a payment to be regarded as authorised, the PSRs explain what steps must be completed. They set out that the payer must have given its consent to the execution of the payment, or a series of payments. And this consent must be given before, or if agreed between parties, after the payment; in the form, and in accordance with the procedure, agreed between the payer and the firm; and can be given via the payee or a payment initiation service provider.

NatWest has shown that all Mr F's payments were initiated in Open Banking – and Mr F accepts he gave the scammer the details to initiate a payment – but were completed by in-app approval on Mr F's registered mobile device. In line with the account terms, this is a way in which Mr F can give NatWest payment instructions.

While Mr F maintains he didn't authorise any of the payments on 13 October 2023, he hasn't been able to explain how the payments were completed by someone else on his registered device. He suggested at one stage maybe a friend made the payments – but it's not clear how they'd have done this. It seems unusual he would make the first payment to this

destination for a scam and then the following morning someone else would choose to access his phone and send four more payments to the same destination. Mr F hasn't been able to explain how a friend would have access to all the security information needed to do this. Practically, this would also mean someone in Mr F's household was working with the scammer that cold-called Mr F. And that despite having full banking access, they only chose to make a small set of payments.

I also have to factor in that Mr F initially said he didn't make any of the payments. So his testimony has changed over time. Ultimately the data I hold shows that Mr F's registered device was used to log-in and approve the payments made in app, using IP addresses previously associated with his genuine account usage. I have no information on a clear point of compromise for Mr F's phone or log-in details to explain how someone else could've made these payments without Mr F's knowledge or consent. So I consider NatWest has fairly deemed them authorised, in line with the PSRs.

As I consider the payments were authorised, I've then considered longstanding regulatory expectations and requirements, and what I consider to be good industry practice. In line with this, NatWest ought to have been on the look-out for the possibility of fraud and made additional checks before processing payments in some circumstances. And the CRM code applies to some situations where a consumer has been scammed. While Mr F hasn't provided evidence to our service he was scammed, NatWest has accepted this was the case.

Our investigator considered Mr F's case under the CRM code, but didn't think he benefited from reimbursement due to exceptions within the code. I agree with these findings, I'll explain why.

One of the exceptions to reimbursement is if Mr F didn't have a reasonable basis for belief in what he was doing. Considering all the payments were sent to the same destination, it seems most likely they were all made for the same purpose as the first payment Mr F accepts he sent, so for the investment opportunity.

Mr F has explained he received an unexpected call late at night advising him of the investment opportunity. He did no research into it, but gave the caller his banking information and approved a £120 payment, expecting to make £1,000. I can't say that on the information he held, Mr F should've considered this was a genuine venture or that he ought to have been satisfied this wasn't a scam. He didn't know who was calling him or check they were genuine and the returns were unrealistic. So I don't think he had reasonable basis for belief in this being a genuine investment opportunity.

In relation to NatWest, the CRM code sets out that, where there's an identifiable scam risk, the firm should provide an effective warning relating to the scam the customer is falling victim to. But the CRM code also has provisions for situations where a firm failed to provide this warning, but it wouldn't have made a difference. In these situations it doesn't require the firm to be liable for failing to provide a warning, as it wouldn't have prevented the loss.

I'm in agreement with our investigator that it wouldn't be fair to ask NatWest to refund Mr F on the basis it didn't provide an effective warning on any of the later payments. Mr F's testimony has changed over time and based on the information available, it still doesn't seem we have the full version of events. It therefore wouldn't be fair to assume any warning would be effective, when we don't know the true situation and/or steps that led to the payments being made.

Due to the above, this means I don't consider Mr F is due a refund under the CRM code. Information provided to NatWest suggests the funds were ultimately used to buy genuine

cryptocurrency. While it tried, NatWest wasn't able to recover the money sent, as a service was provided for the payments. So, considering the information available, I don't find that we can fairly hold NatWest responsible for Mr F's losses in this case, so I don't uphold this complaint.

My final decision

For the reasons set out above, I don't uphold Mr F's complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr F to accept or reject my decision before 14 January 2025.

Amy Osborne
Ombudsman