DRN-5303123

The complaint

Mr H has complained that NATIONAL WESTMINSTER BANK PUBLIC LIMITED COMPANY (NatWest) won't refund money he says he lost to a scam.

What happened

The details of the complaint are well known to both parties, so I will not repeat them again here. Instead, I will focus on giving the reasons 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 investigator's findings for broadly the same reasons. I will explain why.

Firstly, I understand that Mr H's representative has said they would like his complaint to be considered in light of the Contingent Reimbursement Model (CRM). But NatWest are under no obligation to refund the money to Mr H under the CRM Code, as the Code only applies to payments made to another person (which wouldn't have been the case here given the payments were made to an account held in Mr H's own name).

In broad terms, the starting position in law is that a bank is expected to process payments that their customer authorises them to make. It isn't disputed that Mr H knowingly made the payments from his NatWest account. And so, I'm satisfied he authorised them. Therefore, under the Payment Services Regulations 2017 and the terms of the account, NatWest are expected to process Mr H's payments, and he is presumed liable for the loss in the first instance.

However, taking into account the regulatory rules and guidance, relevant codes of practice and good industry practice, there are circumstances where it might be appropriate for NatWest to take additional steps or make additional checks before processing a payment to help protect customers from the possibility of financial harm from fraud.

So, the starting point here is whether the instructions given by Mr H to NatWest (either individually or collectively) were unusual enough to have expected additional checks being carried out before the payments were processed.

While I accept that the amount of money Mr H sent is clearly significant to him, this doesn't in itself suggest a heightened risk of fraud. It's important to note that there is a difficult balance to be struck between firms identifying payments that could potentially be fraudulent and minimising disruption to legitimate payments. Of course, we need to consider that spending habits change, unusual needs arise, and it will be impossible to prevents all fraud without a significant number of genuine payments being delayed considerably and inconveniently.

Mr H says he made four payments totalling £956.87 between 27 August 2021 and 24 November 2021. The payments in question ranged from £214.60 and £279.30. Having reviewed Mr H's accounts statements in the six months prior to the scam, I am satisfied the value of the payments in question were in line with Mr H's usual account expenditure. The payments being disputed here were individually and collectively of a low value with £279.30 being the highest. As such, I don't think payments would've been seen by NatWest as being unusual or out of character for Mr H.

Secondly, Mr H's representative has said, as the payments were going to a single cryptocurrency exchange and given the increasingly high risk associated with cryptocurrency-related fraud, this ought to have triggered NatWest's fraud detection systems. And while I accept, cryptocurrency providers are sometimes used for this purpose, they're also used by many individuals to invest in cryptocurrency legitimately. Because of this, I wouldn't necessarily have expected NatWest to have carried out additional checks before processing the payments simply because they were going to a crypto merchant. And especially considering the value and duration of the payments. But rather, I would expect them to take steps to protect customers that are proportionate to the identifiable risk. I have to bear in mind that if banks such as NatWest were to be expected to intervene with every payment of a similar size to the ones being disputed here - and to crypto wallets in a consumer's own name - it could risk grinding the banking system to a halt.

Lastly, Mr H's representative has said that the frequency and timing of the transactions (over 90 days) should have raised a red flag. I disagree. Based on the payment values and the time between the payments, I'm satisfied it wouldn't be reasonable to have expected NatWest systems to have been triggered by the payments. As explained above the payments were all relatively low in value and the volume of payments were not made in quick succession. As such it didn't appear the payments were being made under pressure and Mr H had sufficient time to reflect and carry out any research he wished to do between each payment. I am satisfied it didn't follow the usual hallmarks of a scam to the extent NatWest ought to have suspected Mr H was at risk of financial harm.

It follows that, while there are circumstances where it might be appropriate for NatWest to take additional steps or make additional checks before processing a payment, for the above reasons, I think at that time it was reasonable for NatWest to assume the payments were being made for legitimate purposes. And so, I think it was reasonable for NatWest to have processed the payments upon receiving Mr H's instructions.

Recovery

I have gone on to consider if NatWest took reasonable steps to try and recover the funds. As, Mr H made the payments via debit card, the chargeback process is relevant here. The chargeback scheme is a voluntary agreement between card providers and card issuers who set the scheme rules and is not enforced by law. A chargeback isn't guaranteed to result in a refund, there needs to be a right to a chargeback under the scheme rules and under those rules the merchant or merchant acquirer can defend a chargeback if it doesn't agree with the request.
Unfortunately, the chargeback rules don't cover scams. So, NatWest would only be able to process chargeback claims against the merchant he paid. The merchant in this case was a genuine cryptocurrency exchange. The service provided by the cryptocurrency exchange would have been to convert or facilitate conversion of Mr H's payments into cryptocurrency. Therefore, they provided the service that was requested.

I appreciate the cryptocurrency was later transferred to the scammer but that does not give rise to a valid chargeback claim against the merchant Mr H paid. As the cryptocurrency

exchange provided the requested service to Mr H and any chargeback attempt would have likely failed.

I also note that Mr H has said he feels compensation is required due to the distress and inconvenience he suffered. And while I don't dispute Mr H would have felt frustrated, distressed and inconvenienced regarding the scam he fell victim to, for the reasons I have provided above, I can't hold NatWest responsible for this.

My final decision

My final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr H to accept or reject my decision before 8 September 2025.

Jade Rowe
Ombudsman