DRN-4423904

The complaint

Mr and Mrs H complain that National Westminster Bank Plc (NatWest) didn't do enough to protect them when they were the victims of a crypto investment scam.

Mr and Mrs H are being supported by a representative, but for ease, I'll refer to Mr and Mrs H throughout this 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 our Investigator, and for largely the same reasons. I've very carefully considered all the evidence provided and I'd like to assure Mr and Mrs H that if I don't mention a particular point, it's not because I haven't considered it, but I've focussed instead on what I believe to be important to the outcome of this complaint.

The details of this complaint are well known to both parties, so I won't repeat everything again here. Instead, I will focus on giving the reasons for my decision.

I should first point out that there was a reasonable expectation on NatWest to protect Mr and Mrs H from financial harm, irrespective of what happened to the money after if left their NatWest account. And so, I'm considering Mr and Mrs H's complaint about NatWest on that basis.

It isn't in dispute that Mr and Mrs H authorised the disputed payments made to their crypto exchange account ('N'). The payments were requested by Mr and Mrs H using the legitimate security credentials provided by NatWest, and the starting position is that banks ought to follow the instructions given by their customers in order for legitimate payments to be made as instructed.

However, taking account of good industry practice, I've considered whether NatWest should've done more to protect Mr and Mrs H.

Mr and Mrs H began trading through a company I'll refer to as ('P'). They were assigned an account manager (the scammer) with who they built up a trusting relationship. Mr and Mrs H made two payments as part of this scam. The first was on 2 November 2022 (£1,300) and the second was on 7 March 2023 (£4,103). NatWest has told us that both payments resulted in a written online warning being sent. Mr and Mrs H said the warning was '***generic and appears before most legitimate payments they make'***.

I don't believe the first payment for £1,300 was sufficiently unusual to have alerted NatWest to the possibility of a fraud or scam. While I accept it is larger than other payments made on Mr and Mrs H's account (which was relatively inactive), it's not an *unusually* large amount in more general terms, and I must bear in mind that it's not uncommon for people to make large one-off payments to a new beneficiary in a normal operating bank account. And so, I

don't think NatWest acted unreasonably by not doing more than providing the written online warning to Mr and Mrs H.

The second payment was arguably more unusual than the first – and was made shortly after Mrs H transferred circa £5,000 into the joint account from her personal account. But the payment amount alone is not the only consideration here, and I don't think there were enough red flags for NatWest to have reasonably expected it to have made further enquiries about this payment before processing it. I say that because the payment wasn't remarkably unusual or of a significantly high value. And it had been four months since Mr and Mrs H made the £1,300 payment, and so there was no *pattern* of payments emerging that would've reasonably caused NatWest obvious concern.

So, taking all this into account, I don't think it was unreasonable of NatWest not to have flagged either of the payments Mr and Mrs H made to 'N' as suspicious and directly intervened before processing them.

Having said that, it's worth pointing out that at the time these payments were made, the prevenance of crypto investment scams meant many firms, including NatWest, recognised that crypto related payments carried a risk of the likelihood of the transaction being related to a fraud or scam. Against that backdrop we'd expect NatWest to provide, at the very least, a *tailored* written warning specific to the risks associated with crypto investment scams. With that in mind, I've carefully considered the online written warning Mr and Mrs H received from NatWest and whether it should've resonated enough with them to alert them to the possible risks. Having done so, I think NatWest's tailored warning was reasonable here. I'll explain why.

I accept Mr and Mrs H's point that the warning is generic, insofar as NatWest has said it is generated when *any* online payment or payment to a new payee is made. But the warning is clearly headed '***Protect your money from fraud and scams'*** and asks the customer to say what the payment is for.

Mr and Mrs H should've selected the 'investing in crypto option' which, if they had, would've generated the following warning:

'WARNING: Thinking of investing in Bitcoin or other cryptocurrency?

Scammers will often contact you offering to help you invest in cryptocurrency … and will offer to guide you through opening a cryptocurrency account. If you cannot access the cryptocurrency wallet or you cannot withdraw money from it, this is a scam and you should stop making payments immediately.

Many cryptocurrency sellers are not registered with the UK Financial Conduct Authority (FCA). We suggest you follow the FCA advice regarding cryptocurrency providers which can be found here …. '

Mr and Mrs H don't think this warning went far enough. In particular, they've said they opened the accounts with 'P' and 'N' themselves and had checked the FCA register and found no negative reviews. Mr and Mrs H don't think the warning is specific to their situation and thought NatWest should've warned about the use of remote access software and unrealistic high rates of return.

I've thought about this carefully, and I do think NatWest's warning was relevant enough to Mr and Mrs H's situation. Mr and Mrs H were contacted by 'P' offering them help to invest. I accept this was prompted by Mrs H making an enquiry with 'P', but I think it's clear the

scammer was *helping* them through the investment process. Mr and Mrs H said the scammer told them they needed to open an account with 'N' to purchase crypto. Again, Mr and Mrs H opened the account with 'N' themselves but were *guided* through that process by the scammer. I'm also mindful that Mr and Mrs H said they questioned the scammer about the need to open an account with 'N' – suggesting they felt some level of concern at this request.

I agree with Mr and Mrs H that the use of remote access software is a clear hallmark of a scam. But I don't think *specific* reference to that not being in NatWest's written warning was a detriment to them. Mr and Mrs H said the scammer directed them to download remote access software. Even if they were unaware of the risks this posed, they've said the scammer told them the software was ***'to let him show them how to manage their accounts with both* ['N' and 'P'] *… eventually he would train* [Mr and Mrs H] *on how to invest themselves for the future'.*** So again, I think it's clear the scammer was *helping* and *guiding* Mr and Mrs H through the investment process, whether that was via the use of remote access software or not.

At the time of the first payment Mr and Mrs H had access to their accounts with 'N' and 'P'. And they've said they were able to make a withdrawal. And whilst it seems there were some negative online reviews about 'P', there was no regulatory FCA warning about 'P' until December 2022. And so, aside from the fact Mr and Mrs H were being helped through the investment process by 'P', I can understand how some parts of NatWest's written warning weren't obviously relevant to Mr and Mrs H's situation at that time.

But I'm mindful of the fact that Mr and Mrs H would've received this warning again when they made the 7 March 2023 payment. By this time, they'd lost contact with the scammer (before being contacted by another representative of 'P') – and I can see from the email exchanges with 'P' that Mr and Mrs H had some concerns about the legitimacy of the investment. There was also now an FCA warning from December 2022 suggesting that 'P' was a clone of a legitimate investment firm.

So, whilst the first warning sent by NatWest in November 2022 was unlikely to have given rise to any concern – and I wouldn't automatically expect further due diligence to take place before another payment is made – in this particular case I think the second warning should've prompted Mr and Mrs H to reflect on the situation they were in and undertake further checks. And if they had, I think it likely they would've realised they were the possible victims of a scam and not proceeded with the £4,103 payment.

Taking everything into account, I don't disagree that Mr and Mrs H have been the victims of a sophisticated and cruel crypto investment scam. But I think NatWest took reasonable action to try and protect them. So, I don't think it's fair or reasonable to hold NatWest accountable for Mr and Mrs H's loss.

My final decision

For the reasons given above, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr H and Mrs H to accept or reject my decision **before 22 December 2023.**

Anna Jackson
Ombudsman