

The complaint

Mr W complains National Westminster Bank Plc (NatWest) didn't do enough to protect him when he fell victim to an investment scam. He would like NatWest to pay him back the money he lost.

What happened

Mr W came across an advert for an investment firm (which I'll refer to as S) on a social media platform in September 2020. It was advertised that he could make £250 a day from trading. Mr W signed up with S, which included providing ID and fulfilling some Know Your Customer (KYC) and Anti-Money Laundering (AML) checks, which he found reassuring. He made an initial investment of just over £200 by card payment. In the following two weeks he made two further debit card payments of £2,020 and £1,717 which were sent to a legitimate crypto exchange.

Mr W realised he'd been scammed when he tried to withdraw his profits but was unable to do so. The phone numbers he'd previously used to contact S had also been blocked.

In February 2021, Mr W contacted NatWest for help in recovering his loss. NatWest explained at the time that Mr W had no chargeback rights in respect of those payments, and so it could not recover his loss.

In August 2022, Mr W complained to NatWest, via a professional representative (who I'll refer to as C), that it had failed to flag the unusual payments from his account and warn him about potential scams. And so, NatWest failed to prevent his loss.

NatWest didn't agree it ought to have prevented Mr W's loss. It explained the payments were not stopped at the time as they did not meet known fraud trends at the time. It had also previously explained why Mr W had no chargeback rights in relation to the payments.

Mr W was unhappy with NatWest's response and referred his complaint to the Financial Ombudsman with support from C. Our Investigator didn't uphold the complaint. He explained that while his investigation had highlighted that Mr W had spoken to NatWest when he attempted to make the second payment, there was no evidence of what was discussed. So, he was unable to assess whether the intervention was proportionate to the identified risk. But he explained that even if the intervention hadn't gone far enough, he needed to assess whether appropriate intervention would likely have prevented the loss. He wasn't persuaded it would have. He noted there were no active warnings about S and that Mr W had invested before and had noted the pattern of this 'investment' matched what he'd seen before. In the circumstances he wasn't persuaded that appropriate intervention would have stopped Mr W from making the payments, so NatWest could not be held responsible for the loss.

C disagreed on Mr W's behalf and asked for an Ombudsman's decision. It said that Mr W's previous investment experience was in stocks and shares, rather than crypto. It also argued that NatWest ought to have noticed the change in Mr W's spending habits, and it should also have detected the use of remote access software and intervened. Our Investigator disagreed

that NatWest ought to have identified that remote access software was being used, as the payments were made by card and therefore not via online banking.

As there has been no agreement, the case has been passed to me to decide.

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'm not upholding this complaint and for largely the same reasons as our Investigator. I realise this will be extremely disappointing to Mr W. I don't underestimate the financial and emotional damage falling victim to this scam has had on him. But for the reasons I'll go on to explain I don't think NatWest has acted unfairly or unreasonably.

I'm sorry to hear Mr W was the victim of a sophisticated scam. I can appreciate why he wants to do all he can to recover the money he lost. But I can only direct NatWest to refund his losses if it can fairly and reasonably be held responsible for them.

It is accepted that Mr W authorised each of the card payments from his NatWest account. So, although he didn't intend the money to go to the scammers, under the Payment Services Regulations 2017 and the terms and conditions of his account, Mr W is presumed liable for his loss in the first instance. And under the terms and conditions of the account, where a valid payment instruction has been received, NatWest's obligation is to follow the instructions Mr W provides.

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 its customers from the risk of financial harm from fraud. But NatWest would only fairly and reasonably need to intervene and ask more questions about the payment if an instruction was sufficiently unusual or uncharacteristic for the account. Ultimately, there is a balance to be struck between identifying payments that could potentially be fraudulent and minimising disruption to legitimate payments.

Like our Investigator, given its relatively low value, I don't think NatWest needed to intervene before processing the first payment as there was no reason to suspect, on the basis of that payment alone or anything else NatWest knew at the time, that Mr W was at risk of financial harm from fraud.

There is evidence that NatWest had some contact with Mr W before the second payment was processed. We have been provided with part of a phone recording in which Mr W explains his account has been blocked following an attempt to make a £2,000 payment – given the date of this call I've assumed it relates to the £2,020 payment. Unfortunately, NatWest has been unable to recover the second half of the call where the discussion with the fraud team took place. We asked Mr W for his recollections of this phone call but to date we've received no answer to our enquiries. I can only assume that Mr W is either unwilling or unable to share his recollections of this conversation.

In the circumstances it's unclear what prompted NatWest to contact Mr W. Given what NatWest knew about the payment, I would not necessarily have expected the final two payments to have triggered its systems due to the activity appearing unusual or suspicious. I have considered whether NatWest may have wanted to carry out further checks to confirm it was Mr W who authorised the payment, or it may have been triggered for a scam check. In either event, without any clear evidence of what was discussed I can't safely conclude the intervention was proportionate to the risk identified. But I must also consider whether

NatWest's potential failure to provide an appropriate warning resulted in Mr W's loss, and I'm not persuaded it did.

While I accept there were features of the proposed investment with S that may have given NatWest cause for concern that it was a scam – in particular, the promotion through social media and the fact that there was a third party involved – there was no specific evidence that confirmed that it was indeed a scam at the time – for example warnings from the FCA or other regulatory bodies.

I have also considered C's suggestion that NatWest ought to have detected the use of remote access software and therefore done more to stop the payment, but I disagree. I have seen no evidence to demonstrate that NatWest was able to detect the use of remote access software in 2020, nor was it under a specific obligation to do so. As our Investigator also explained, given that the payments were made by card there was also less opportunity for NatWest to detect the use of remote access software as the payment wouldn't have been made from Mr W's online banking. I also wouldn't have expected NatWest to have necessarily asked Mr W whether remote access software had been downloaded when it did speak with him.

I must therefore weigh up whether reasonable intervention from NatWest, would have resonated with Mr W more so than his own research and experience of what was going on. And I'm not persuaded it would have.

Mr W has explained that at the time of making the payments he had researched S and had only found positive "5 star" reviews online. He was also reassured by the way S was presented online - he noted the website looked professional, with lots of information about the company and trading, including graphs and trends. The person he spoke with also sounded professional and knowledgeable, and had carried out KYC and AML checks, which again appeared plausible and legitimate. He was also aware of background noise when speaking with the scammer that sounded like a normal office environment.

Mr W has also explained that he saw immediate profits following his first payment, which were reflected on his investment platform balance, which would no doubt have reassured him that the investment was legitimate and achieving what he'd been promised.

When NatWest intervened, I'd have expected it to use the opportunity to understand the nature of the payment Mr W was attempting to make. Once it understood that Mr W was attempting to make a crypto investment, I would have expected it to warn him about the hallmarks of a crypto investment scam and encourage him to carry out additional due diligence. I would not have expected it to stop the payment as there wouldn't have been sufficient reason to think Mr W was at significant risk of financial harm from fraud. So, it would have been up to Mr W whether to continue with the payment or not.

Having given it careful consideration, and in the knowledge that I don't have the full facts of what was discussed with NatWest, I'm not persuaded that intervention from NatWest would have stopped Mr W from making future payments. I think when balanced against all the information he had gathered himself, as well as the lack warnings or adverse information about the broker at the time, Mr W would have felt reassured that the investment was legitimate, as any further research would've been unlikely to yield any results that would have led him to believe he was falling victim to a scam.

So, whether NatWest did enough when it intervened on the second payment or not, I'm not persuaded it would have prevented Mr W's loss. As such, I can't reasonably hold it responsible for his loss.

I've considered whether, on being alerted to the scam, NatWest could reasonably have done anything to recover Mr W's losses, but I don't think it could. The only possible option for recovery here, given the payments were made by debit card, would have been via chargeback claims. But given these payments went towards purchasing crypto from legitimate firms, I don't think chargeback claims would have been successful as Mr W received the service he paid for. Mr W also first notified NatWest of his loss in February 2021, so any potential chargeback claims would also have been out of time. As such, I think it was reasonable in the circumstances that NatWest didn't raise chargeback claims here.

I have a great deal of sympathy for Mr W and the loss he's suffered. But it would only be fair for me to direct NatWest to refund his loss if I thought it was responsible – and I'm not persuaded that this was the case. For the above reasons, I think NatWest has acted fairly and so I'm not going to tell them to do anything further.

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 Mr W to accept or reject my decision before 4 January 2024.

Lisa De Noronha
Ombudsman