DRN-6022617

The complaint

Mr S complains that NATIONAL WESTMINSTER BANK PUBLIC LIMITED COMPANY (NatWest) is refusing to refund him the amount he lost as the result of two scams.

Mr S is being represented by a third party. To keep things simple, I will refer to Mr S throughout my decision.

What happened

The background of this complaint is well known to all parties, so I won't repeat what happened in detail.

In summary, Mr S has explained that he has fallen victim to two separate scams.

Scam 1

In March 2024 Mr S was contacted by a company I will call "X" explaining the regulators had located Bitcoin belonging to him to the value of $90,000 (Mr S had fallen victim to a scam previously that had resulted in a loss of around £5,000).

X would help recover the funds for Mr S and would charge a commission to do so. Remote access software was also used so X could guide Mr S through different processes.

Throughout the process of recovering the funds Mr S was introduced to several people associated with X and given multiple reasons as to why he would need to make payments via cryptocurrency to release the funds.

After making multiple payments as requested by X, Mr S realised he had fallen victim to a scam.

Scam 2

In June 2024 Mr S was contacted by a company I will call "Y" explaining that it had also located Bitcoin belonging to him. Y requested a small initial payment to establish a link to Mr S's account. Y then explained that Mr S's funds had been sent and were pending but Y also convinced Mr S to invest further stating that Bitcoin were having an event and prices were likely to increase.

While in contact with Y Mr S explained that he had funds stuck in an investment with X. Y offered to help but explained a fee of £15,000 would be payable. Mr S paid the fee via Bitcoin in July 2024.

Mr S was then advised he would have to pay multiple fees and taxes before he could receive funds promised by Y,

Mr S was required to open an account with what appeared to be a genuine cryptocurrency exchange where funds appeared to be deposited. But the exchange then also requested further payments before any funds could be released.

Mr S later found that the scammers were impersonating a well-known cryptocurrency exchange and he had not been making payments to a legitimate company.

Mr S has disputed the following payments made from his NatWest account in relation to the scam:

Payment	Scam	Date	Payee	Payment Method	Amount
1	1	13 June 2024	XChainger (Crypto)	Transfer in Branch	£1,000
2	1	14 June 2024	XChainger (Crypto)	Transfer in Branch	£4,990
3	1	17 June 2024	Nieto Candela Soleda (Crypto)	Transfer in Branch	£4,237
4	1	18 June 2024	XChainger (Crypto)	Transfer in Branch	£9,500
5	2	17 July 2024	CoinCorner	Transfer	£1,000
6	2	30 July 2024	CoinCorner	Transfer	£6,202
7	2	15 August 2024	CoinCorner	Transfer	£5,000
8	2	16 August 2024	CoinCorner	Transfer	£20,000
9	2	6 September 2024	CoinCorner	Transfer	£13,600
10	2	7 October 2024	CoinCorner	Transfer	£5,250

Our Investigator considered Mr S's complaint and didn't think it should be upheld. Mr S disagreed, so this complaint 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.

It has not been disputed that Mr S has fallen victim to cruel scams. The evidence provided by both Mr S and NatWest sets out what happened. What is in dispute is whether NatWest should refund the money Mr S lost due to the scams.

Recovering the payments Mr S made

Mr S made payments into the scam via transfer. When payments are made by transfer NatWest has limited options available to it to seek recovery. In any event the payments Mr S made were not made directly to the scammer instead they were used to purchase cryptocurrency. As it took further steps for those funds to end up in the hands of the scammer any attempts at recovery would have no prospect of success.

Should NatWest have reasonably prevented the payments Mr S made?

It has been accepted that Mr S authorised the payments that were made from his account with NatWest, albeit on X and Y's instruction. So, the starting point here is that Mr S is responsible.

However, banks and other Payment Services Providers (PSPs) do have a duty to protect against the risk of financial loss due to fraud and/or to undertake due diligence on large transactions to guard against money laundering.

The question here is whether NatWest should have been aware of the scams and intervened when the payments were being made. And if it had intervened., would it have been able to prevent the scams taking place.

I can confirm that NatWest did intervene on more than one occasion.

Before the successful payments were made Mr S attempted payments in relation to the scams from his NatWest account.

On 23 May 2024 a call between Mr S and NatWest took place to discuss a payment that was being attempted for £3,000. Mr S incorrectly explained that he was making a payment to a friend he had known for a long time that needed help. Mr S said he didn't want the payment to be delayed.

NatWest explained that it could see screensharing software had been installed on Mr S's device, but Mr S said this must have been something to do with his wife.

Throughout the call Mr S confirmed on several occasions that the payment was being made to a friend. This payment was not processed, and NatWest explained the reason was due to the system flagging a scam concern. Mr S continued to make payments in relation to the scams from accounts he held at other providers.

It is difficult to know exactly how the conversations took place when Mr S made payments via a branch visit. Although NatWest has provided some branch notes available from the time Mr S made payment 4.

From the notes it's clear that Mr S confirmed:

- The payment was being made in relation to a house purchase
- The payment was going to an existing payee
- He had not been asked to make an urgent payment or received a request to do so

It's also clear that Mr S was required to provide proof of his identification before the payment was processed.

On 4 July 2024 NatWest intervened again when Mr S attempted to make a payment in relation to the scam. NatWest confirmed it was unable to make the payment as it was related to cryptocurrency investment, and it had seen too many scams related to cryptocurrency.

Overall, I think it's clear that Mr S was determined to make the payments in relation to the scam and give incorrect information to NatWest to have the payments processed.

Mr S was not making a payment to a friend, he had downloaded AnyDesk and payments were not being made in relation to a house purchase.

While I think NatWest should have intervened further on other occasions and questioned Mr S when he attempted to make payments from his NatWest account, I don't think this would have made a difference.

When Mr S was unable to make payments from his NatWest account and, other accounts he held elsewhere he discussed the difficulties with the scammer and found an alternative way to make the payments. Mr S also gave incorrect information to his other account providers on multiple occasions to have payments processed.

Overall, I don't have enough to say that Mr S would have provided any mor accurate information to NatWest had it intervened further than it did, or that any further intervention would have prevented Mr S's loss.

With the above in mind, I don't think NatWest missed an opportunity to prevent the scams

and it is not responsible for Mr S's loss.

Mr S has told us he was vulnerable at the time the payments were made but it is my understanding that NatWest was not made aware of any vulnerabilities that could have affected Mr S's ability to make sound decisions. So, I can't reasonably have expected NatWest to have taken any vulnerabilities into account when the payments were made.

My final decision

I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr S to accept or reject my decision before 9 April 2026.

Terry Woodham
Ombudsman