DRN-5970767

The complaint

Mr and Mrs D complain that National Westminster Bank Public Limited Company (NatWest) won't refund the money Mr D lost to an investment scam.

What happened

The detailed background to this complaint is well known to both parties. So, I'll only provide a brief overview of some of the key events here.

In late January 2025, Mr D came across a social media advertisement promoted by a well-known businessman which led him to join a trading chat group. This group was led by a well-known professor and Mr D was contacted by Person J (a scammer) and she led him to believe she was the professor's assistant.

Person J explained and presented the Company P trading programme and platform to Mr D. Mr D thought it was legitimate, and he decided to purchase cryptocurrency, which he was led to believe would generate profits and double his funds within a short period.

Mr D could see large profits that group members said they were making and after some initial investments and profit, he was persuaded to increase his investment. He was told he could make up to 50% profit and to make payments through the following:

- An online payment system – Company P
- Crypto companies – Company M, Company F and Company S

From his Bank L account, he made nine payments to Company M totalling £1,658.84 between 10 February 2025 and 14 March 2025. These payments appear to have been refunded.

From his NatWest account, he made the following four payments (3 to Company F and 1 to Company P), totalling £5,950, between 24 March 2025 and 28 March 2025:

Payment Number	Date / Time	Payment Method	Payee	Amount
1	24/3/25 21:49	Faster Payment	Mr D's account with Company F	£1,000
2	25/3/25 16:06	Faster Payment	Mr D's account with Company F	£1,500
3	25/3/25 16:35	Faster Payment	Mr D's account with Company F	£2,500
4	28/3/25 14:21	Card Payment	Mr D's account with Company P	£950

Mr D realised it was a scam when the promised returns never came, communications stopped, and other members reported losing money.

Mr D complained to NatWest, seeking a refund of his loss, as he considers they should've been monitoring unusual high-risk payments and issuing strong warnings. However, NatWest rejected his complaint and claim as the scam payments were made through another account in his name and they weren't the point of loss.

Mr D brought his complaint to our service. However, our investigator discovered that Bank L put a human intervention in place on a £5,000 payment attempted by Mr D on 22 March 2025. Although he considered that automated intervention would've been proportionate on the amounts Mr D paid through his NatWest account, as he'd received a strong intervention and had chosen to ignore this, he didn't think the scam could've been prevented.

Mr and Mrs D disagree with the view of our investigator and made a number of points for an ombudsman to consider. These included the following:

- Whatever may have occurred with Bank L, NatWest should've intervened to protect Mr D and there is no evidence that they did.
- They question whether Bank L considered it to be a clear scam.
- NatWest haven't provided evidence that it attempted card scheme payment recovery remedies (for payment 4).
- A NatWest intervention would've changed the outcome.

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, although I'm very sorry to hear that Mr D has been the victim of this cruel investment scam and he and Mrs D have lost a significant amount of money here, I'm not upholding this complaint. I'll explain why.

I should first say that:

- Although I've read and considered everything Mr and Mrs D have said, I won't be responding to every point individually. If I don't comment on any specific point, it's not because I've not considered it but because I don't think I need to comment on it in order to reach the right outcome.
- In making my findings, I must consider the evidence that is available to me and where evidence is incomplete, inconsistent or contradictory, as some of it is here, I must reach my decision on the balance of probabilities – in other words, what I consider most likely to have happened in light of the available evidence and wider circumstances.
- Although the voluntary CRM code was in place in 2024, and NatWest were signed up to it, I'm satisfied the payments were made to an account in Mr D's own name. Unfortunately, this means the payments aren't covered by the code.
- Regarding recovery, as the payment went to other accounts and then to the scammer in crypto, I don't think NatWest could've been expected to recover Mr and Mrs D's funds.
- Regarding a chargeback for payment 4 (by card) I would also only expect NatWest to raise a chargeback if it was likely to be successful. But, as correctly explained by our investigator, chargeback reasons unfortunately don't apply here as it can't be said that the payment wasn't authorised or the goods/services weren't received.
- The Payment Services Regulations 2017 (PSR) and Consumer Duty are relevant here.

  PSR

Under the PSR and in accordance with general banking terms and conditions, banks should execute an authorised payment instruction without undue delay. The starting position is that liability for an authorised payment rests with the payer, even where they are duped into making that payment.

I'm satisfied that Mr D authorised the payments here. However, in accordance with the law, regulations and good industry practice, a bank should be on the look-out for and protect its customers against the risk of fraud and scams so far as is reasonably possible. If it fails to act on information which ought reasonably to alert a prudent banker to potential fraud or financial crime, it might be liable for losses incurred by its customer as a result.

Banks do have to strike a balance between the extent to which they intervene in payments to try and prevent fraud and/or financial harm, against the risk of unnecessarily inconveniencing or delaying legitimate transactions.

So, I consider NatWest should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks such as anti-money laundering and preventing fraud and scams.
- Have systems in place to look for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which banks and building societies are generally more familiar with than the average customer.
- In some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

Consumer Duty

Also, from July 2023, NatWest had to comply with the Financial Conduct Authority's Consumer Duty which required financial services firms to act to deliver good outcomes for their customers. Whilst the Consumer Duty does not mean that customers will always be protected from bad outcomes, NatWest was required to act to avoid foreseeable harm by, for example, operating adequate systems to detect and prevent fraud.

With the above in mind, I looked closely at the file and four payments Mr D made to determine if NatWest recognised a risk of financial harm and took proportionate action.

When looking at the file, I found some information to be both incomplete and contradictory. I say this because:

- Bank C is a clearing bank for a variety of financial institutions, and it isn't possible to know if NatWest knew that Bank C were clearing payments 1 to 3 on behalf of a crypto company (Company F).
- Mr and Mrs D says Mr D didn't receive any warning from NatWest and holds them responsible for their loss. NatWest though have provided information that Mr D would've received a warning on his banking app; however, they can't evidence the payment reason Mr D selected and the warning they subsequently gave him. Also, there is information from Mr D's dialogue with the scammer and interactions with Bank L, that after being encouraged to ignore bank warnings, he disregarded what Bank L said.

Payments 1 (£1,000) and 2 (£1,500)

Even if NatWest knew that payments 1 and 2 were going to a crypto company and therefore had a heightened risk, I wouldn't have expected them to view these as out of character, unusual or suspicious enough to intervene. This is because Mr and Mrs D had previously made payments to another crypto company (Company E), crypto payments are very common, and the amounts and preceding credits weren't significantly high or different to other account entries. Also, there wasn't any concerning pattern such as the payments being made within minutes of each other.

Payment 3 (£2,500)

Although this NatWest payment wasn't for a particularly high amount, it was the second payment made in a short space of time to Company K on 25 March 2025. It took his Company K payments to £4,000 on 25 March 2025. So, if NatWest knew this payment was going to a crypto company, I would've expected to have seen an intervention.

But, importantly, bearing in mind that the payment amount wasn't particularly high and that Mr and Mrs D had made previous crypto payments, I would've also expected this to be in the form of a tailored warning and education about crypto investments and scams.

Payment 4 (£950)

Regarding payment 4, Company P isn't associated with crypto payments. It is a well-known payment platform that allows users to sell and purchase products, manage transactions and receive money. Also, the amount wasn't inconsistent with other spend. So, I don't think NatWest would've seen this payment as being either unusual, suspicious or connected to payments 1, 2 or 3.

Although Mr D says he didn't receive such a tailored warning, and education, about crypto investments and scams on payment 3, I think, more likely than not, that:

- Prior to payment 3 (when he made payment 1) NatWest required him to select a payment reason and, if he'd selected the option '*Investing in cryptocurrency'*, he would've been given the following strong warnings:
    - *'Investing in Crypto Currency. Warning: Criminals are increasingly scamming people by setting up fake crypto accounts or taking control of their accounts.*
    - *Scammers will often contact you offering you help to invest in cryptocurrency (e.g. Bitcoin) 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.*
    - *Have you checked the cryptocurrency provider is on the Financial Conduct Authority Register?.*
    - *It is unusual for genuine cryptocurrency investment opportunities to be on social media, such as Instagram. If you think you have found an opportunity or been approached with one, this maybe a scam, please follow the Financial Conduct Authority advice below before proceeding'.*

  This is because Company F was a new payee and NatWest have provided evidence that when their customers set up a new payee, they are required to select a reason from a set of payment reasons with each reason triggering specific educational information and warnings.
- Mr D gave an incorrect reason that didn't apply to his payment and he therefore got the wrong type of warning. And this negated NatWest's fraud and scam prevention system.

  I say this because Mr D can't recall seeing any crypto investment warnings. Also, Mr

D's dialogue with Person J shows he was disappointed that the Bank L payment was blocked. And Person J was influencing him to make more payments and to disregard banks warnings. In addition, Mr D was making the payments after Bank L's human intervention where I found Bank L gave him very strong warnings, education and advice. Furthermore, during this intervention Mr D consulted with his family and decided to discontinue the Bank L payment due to joint reservations on the risk.

If Mr D had inputted the correct payment reason, I'm satisfied he would've received tailored warning, and education, about crypto investments and scams (which would've been directly relevant to the scam he was experiencing) at an earlier point.

But, importantly here, even if he'd received this, Bank L had already put in place a much stronger type of intervention. This is because he made a much higher payment of £5,000. In a human intervention, with a fraud and scam specialist, Bank L told Mr D (who consulted with Mrs D) that there was a strong scam risk. This stronger intervention included the following:

- Research of Company P.
- Pointing out concerning information, which was a lack of internet presence and poor trust site reviews from customers unable to withdraw funds. Also, he said he would send links on what he could see about Company P together with scam advice.
- Questioning Mr D about who he was paying, his ability to withdraw and whether he had control over the wallet and explained the risk and how scammers operate.
- Ascertaining Mr D hadn't made any withdrawals and urging Mr D to take action, including making sure he knew who he was dealing with and whether they were regulated. He also gave educational information pointing out that if they are promising you something too good to be true it probably is.
- Pointing out that Mr D (who wanted to see if it worked) risked losing his £5,000 if he proceeded.

So, even with stronger and better intervention than he would've received from NatWest (if he'd selected what I consider to be a correct and proportionate intervention option) before the release of payment 1, Mr D still decided to proceed.

I recognise the cunning tactics and manipulation of the scammer and that this caused Mr D to be under her spell, think he'd made a profit (which would further increase) and trust Person J over his bank (Bank L). So, I in no way blame him for continuing to make the payments through NatWest. However, considering the above and all the information on file, I don't think it would be fair or reasonable to hold NatWest responsible for his loss and require them to make a refund.

My final decision

For the reasons mentioned above, my final decision is not to uphold this complaint against National Westminster Bank Public Limited Company.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs D and Mr D to accept or reject my decision before 29 December 2025.

Paul Douglas
Ombudsman