DRN-5832539

The complaint

Mr K complains that National Westminster Bank Plc (NatWest) won't refund the money he lost to an investment scam. Mr K is represented in this complaint, but I'll refer to him as it's his complaint.

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 or around August 2024, Mr K was contacted on a social networking service by X (the scammer) about an investment.

He started to speak to X on a messaging app, who said she was a financial analyst and a business mentor. X introduced Mr K to a broker called Company Z and Investment Platform P. Mr K could see realistic investment graphs and he thought they looked official and legitimate. Also, he could see people making money from bitcoin.

Mr K says he researched cryptocurrency, Company Z and the investment platform and then started to invest. He explains that he could see profits on Platform P on a daily basis, which gave him further reassurance that the investment was legitimate. Also, each day he would speak to X and Company Z. Mr K started to build a relationship and trust with X, who said she was religious, and he was convinced she genuinely helping him.

Mr K had accounts with NatWest, Bank B, Bank H and Firm R and he transferred funds from these accounts to his accounts with crypto exchanges and then onto the scammers' crypto account.

The scammers' tactics were:

- To show Mr K that he was making significant profits and that to gain higher profits, he needed to pay them fees.
- For X to encourage him to invest and, when he doubted the investment and got frustrated and annoyed, to persuade him that it was legitimate and to pay more and more fees until he had given them all his money. Also, to persuade Mr K, X would explain the fees, withdrawal issues and how successful his investment had become. Also, when he struggled to pay the fees, she agreed to make fake contributions.

Under the spell of the scammers Mr K transferred the following amounts between 13 August 2024 and 24 October 2024:

- £12,500 from Bank R – 13 to 23 August 2024
- £17,804 from Bank H – 16 August 2024 to 24 September 2024
- £18,550 from NatWest – 9 to 11 September 2024
- £36,400 from Bank B – 13 September 2024 to 24 October 2024

The £18,550 Mr K paid from his NatWest account went to his account with Company C and was comprised of the following amounts:

Payment Number	Date	Payment Method	Beneficiary	Amount (£)
1	9 Sept 2024	Faster payment	Mr K account with Company C	2,500
2	9 Sept 2024	Faster payment	Mr K account with Company C	3,700
3	9 Sept 2024	Faster payment	Mr K account with Company C	250
4	10 Sept 2024	Faster payment	Mr K account with Company C	3,250
5	10 Sept 2024	Faster payment	Mr K account with Company C	3,250
6	11 Sept 2024	Faster payment	Mr K account with Company C	5,300
7	11 Sept 2024	Faster payment	Mr K account with Company C	300
Total				**18,550**

Mr K realised he'd been scammed at the point he thought his investment was worth £785,000. He wanted to withdraw £100,000 but couldn't afford fees which had a deadline.

Mr K complained to all four banks.

In his complaint to NatWest, in which Mr K asked for a refund of his £18,550 loss and interest, he said the above payments *'were completely unusual and out of character, and had the relevant interventions been conducted, the scam would have been stopped and the loss prevented'.*

NatWest rejected Mr K's claim. They said:

- They did monitor his payments but didn't have concerns.
- *'As the payments were made to an account in the customer's name, we would not look to review any reimbursement under the APP, CRM codes or under BSI PAS'.*

Mr K was dissatisfied with NatWest's response and brought his complaint to our service. However, upon listening to call recordings of interventions from Bank H and Bank B our investigator didn't think NatWest should reasonably have been expected to prevent the scam.

As Mr K remains dissatisfied his complaint has been referred to me to look at.

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.

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 K has been the victim of this cruel investment scam and lost a significant amount of money, I'm not upholding this complaint. I'll explain why.

I should first say that:

- Although NatWest is a signatory of the Lending Standards Board's Contingent Reimbursement Model ("CRM") Code which requires firms to reimburse customers

who have been the victim of a scam in most circumstances, I'm satisfied this code doesn't apply here. This is because the CRM Code sets out the following:

Under 'DS1(2) (a)' the scope of what the CRM Code covers in relation to authorised push payment ("APP") fraud in instances where: "(i)The Customer intended to transfer funds to another person, but was instead deceived into transferring the funds to a different person; or (ii) The Customer transferred funds to another person for what they believed were legitimate purposes but which were in fact fraudulent."

And the payments Mr K made from his NatWest account went to an account in his own name. So, they aren't covered by or within the scope of the CRM Code. This is because Mr K wasn't paying 'another person'.

- In making my findings, I must consider the evidence that is available to me and use it to decide what I consider is more likely than not to have happened, on the balance of probabilities.
- 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. There's no dispute that Mr K made the payments here, so they are considered authorised.

  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 are generally more familiar with than the average customer.
  - In some circumstances, irrespective of the payment channel used, have taken additional steps, or make 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 PSR and Consumer Duty in mind I first considered whether:

NatWest should've recognised Mr K was at risk of financial harm from fraud and put in place proportionate interventions?

I found that NatWest did put a strong tailored automated intervention in place, having recognised that Mr K's first payment, for £2,500 on 9 September 2024, was going to a high-risk crypto exchange.

I say it was strong as it was about crypto payments and bitcoin and was directly relevant to the scam to which Mr K had been making payments since 13 August 2024.

It showed a red warning triangle and, in large bold print said:

- '*Criminals are increasingly targeting people by setting fake crypto accounts'.*

This was followed by messages that:

- *'Scammers will often contact you offering to help you invest in cryptocurrency (e.g. Bitcoin') and will 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.*

And below the above messages blue wording said:

- '*Cryptocurrency investment fraud'*

Then, messages, in large font, said:

- *'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'.*
- *'If you think you have found an opportunity or been approached with one, this maybe a scam, please follow the Financial Conduct Authority guidance before proceeding'.*

They then provided links for this guidance.

Despite these messages being directly relevant to Mr K's situation was and Company Z and Investment Platform P not being approved by the FCA, Mr K went ahead and authorised the payment. Then, later on the same day, he made a second payment to the scammers for a larger amount of £3,700.

I recognise NatWest process thousands of payments each day and have to strike a balance between the extent to which they intervene in payments to try and prevent fraud and/or financial harm. However, this was the second consecutive payment Mr K made for a high-risk crypto investment taking his payments for the day to £6,200, and he had also just moved funds (for the same two amounts) into his account from another bank.

As NatWest knew about the risks of multi-stage crypto scams, I think they should've seen this as unusual, with a heightened risk of fraud, and looked to probe what was going on to check Mr K wasn't at risk of financial harm.

I can't see NatWest put in place an intervention with a fraud and scam agent and if a bank doesn't question payments that might be at risk, then it can't fulfil its duty to protect customers.

I then considered:

What would've happened if NatWest had put in place an effective intervention with one of their fraud and scam agents and whether this would've prevented Mr K's loss?

The payments Mr K made to the scammers, from his four accounts, took place over an eleven-week period between 13 August 2024 and 24 October 2024 and there were four intervention calls with fraud and scam agents:

- Bank H intervened on 24 August 2024 (week 2 of the 11-week period).
- Bank B intervened on 12,13 and 17 September 2024 (week 5 and 6 of the 11-week period).

Having listened to these intervention calls, which overall I found to be strong, and taken note of the above mentioned relevant NatWest automated warning and an irrelevant automated from Bank B (because Mr K said he was paying family and friends), I'm not persuaded that NatWest would've been able to detect, unravel the scam or stop Mr K's loss, even if they had put an intervention in place.

An intervention shouldn't be an interrogation; it should be suitable questions designed to unearth a potential scam and establish if the customer is at risk of financial harm.

Although there isn't any evidence that coaching took place to reduce payments and counteract interventions and Mr K says he *'had no reason to lie or evade questions from the bank'*, I considered this to be a possibility as:

- I found Mr K wasn't truthful to both Bank H and Bank B.
- Mr K was having daily conversations with the scammers.
- I noted that in his dialogue with X, Mr K discussed the banks he was using and after the intervention call with Bank B concluded on 13 September 2024 he said to X:
    - '*What a nightmare. I feel like a criminal all the questions!'*

So, although I don't know if the scammers were coaching Mr K, when listening to the call recordings, I considered whether the agents were alive to the risk of coaching.

In summary, on the calls:

- Mr K consistently received educational information and warnings on crypto investment scams. These included the following:
    - Scammers approach people on social media and the scams include fake brokers, fake platforms and trading accounts.
    - Scammers show realistic graphics illustrating profits together with group chats or messages from people making profits.
    - The profits will be too good to be true. Scammers pressurise victims to pay more and more money in extortionate fees to access high profits.
    - Even when victims can't access fake profits, and they think it may be a scam, they often struggle to accept the reality and continue to pay more.
    - Scammers tell and coach victims to move funds between accounts and to lie to their banks.
    - Banks continue to see a rise of investment scams with crypto and bitcoin being higher than normal risk. These are volatile due to lack of regulation and therefore due diligence and checking with the FCA is important.
    - Crypto investors should be prepared to lose all their funds.

    Most, and perhaps all, of the above scam warnings applied to Mr K. He had been approached by social media, he thought he had a broker, he was surprised the

profits were so large (commenting to X that '*When it's too good to be true it usually is'*), he was getting annoyed and frustrated with the extortionate fees and being asked to make more and more payments. At a number of stages, he thought he was being scammed but due to the spell X had over him and the amount of money he had invested had he ignored his own misgivings. Also, he appears to have had misgivings over the investment as he tells X *'Lots of people have told me that this company are scammers'.*

Yet when repeatedly asked questions about whether any of the above applied to what he was doing he said it didn't and he consistently gave false answers saying he was acting alone after a well-known male friend had given him advice.

Regarding the warnings about the high risk of losing all his money, Mr K said he understood and accepted all the risks.

- Mr K faced lots of probing questions, particularly on the Bank H call and Bank B call of 13 September 2024. I could understand Mr K's above comments about how he felt about the Bank B call as this lasted thirty minutes and it was a very strong call in terms of education, warnings and probing. I think the Bank B agent may have been suspicious that Mr K was being coached as he repeatedly asked him if anyone was asking him to lie and told him about the importance of giving honest answers to his questions. However, on all the calls Mr K was insistent that no one was telling him to lie, maintains this in his complaint, and it isn't illegal for customers to trade in crypto.

  The agents asked both open and closed questions. I found Mr K also gave false and misleading answers to the following questions:

  - Why was he investing in bitcoin? How was he introduced to it?
    - He consistently said it was a long-standing friend who was making money from bitcoin through a crypto exchange company. And when probed further about his friend, how he knew him and how he communicated with him, he gave false answers.
  - Was any third party advising or helping him? Did he have an investment company and broker acting on his behalf? Is he paying exorbitant fees? What research had he done?
    - He consistently said no, which also wasn't the case.
    - Also, he'd done his own research following his friend's advice.
  - How does he communicate with a third party or investment company? How does he know the investment company? How does he make withdrawals? Is someone saying you can make loads of money? Who is advising you?
    - He again consistently said it was just him acting on his friend's recommendation.
  - He was repeatedly told that for the bank to protect him they needed him to be honest and asked if anyone was telling him to lie or manipulating him. And that only a scammer would do so.
    - He consistently said no to these questions.

  Mr K was asked a number of other questions including why he was transferring funds between his accounts and whether he was gaining high returns in a short space of time.

  Overall, I found the interventions to be strong. I think there could've been some more probing about his answer to the high returns in a short space of time question and two of the calls were at risk of becoming interrogations.

However, whatever further questions the agents asked, I don't think Mr K was going to give them any information on what was really happening.

Having considered the above, although I think NatWest should've put a human intervention call in place, I don't think Mr K would've listened to their warnings and they wouldn't have been able to uncover the scam at that time even if they had probed further.

Finally, with regards to recovery, Mr K's funds were paid into a crypto wallet and then sent on to the scammer, so unfortunately there was no realistic opportunity for NatWest to recover the funds.

I realise the outcome of this complaint will come as a great disappointment to Mr K and I'm very sorry he has lost a significant amount of money here. But, for the reasons I've explained, I won't be upholding this complaint and asking NatWest to make any 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 Mr K to accept or reject my decision before 20 October 2025.

Paul Douglas
Ombudsman