

The complaint

Mrs J is complaining about National Westminster Bank Public Limited Company because it declined to refund money she lost as a result of fraud.

What happened

Sadly, Mrs J fell victim to a cruel job scam after she was contacted online. The role required her to complete sets of online reviews that she was required to pay to access and for which she expected to receive commission on completion. Between July and October 2025, she used her NatWest account to make the following payments that were ultimately lost to the scam:

No.	Date	Amount £	Payee	Method
1	18 Jul	37	Money transfer service 1	Card
2	19 Jul	200	Money transfer service 1	Card
3	19 Jul	559	Money transfer service 1	Card
4	19 Jul	1,461.99	Money transfer service 2	Card
5	27 Aug	205.98	Cryptocurrency exchange	Card
6	2 Oct	650	Cryptocurrency exchange	Card
7	10 Oct	900	Cryptocurrency exchange	Card
8	12 Oct	308	Cryptocurrency exchange	Transfer

Mrs J called NatWest on 20 July to report the scam but was told the bank couldn't help recover her money as it went to accounts in her own name. She was told she should contact the money transfer services she'd used instead.

After this, she says she was convinced by the scammers to make further payments in the belief that she'd be able to withdraw her earnings once outstanding tasks were completed.

Our investigator didn't recommend the complaint be upheld. He didn't feel there were sufficient grounds for NatWest to have suspected the payments were part of a scam or that it should have intervened to stop them.

Mrs J didn't accept the investigator's assessment. She says she was in a vulnerable mental state at the time and was coerced by the scammers, including threats of legal action, into making payments 5 to 8. She says NatWest should have realised the payments she was making were unusual and done more to protect her from foreseeable harm. But instead she wasn't given any warnings about fraud and scams.

The complaint has now been referred to me for review.

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've reached the same overall conclusions as the investigator. I haven't necessarily commented on every single point raised but concentrated instead on the issues I believe are central to the outcome of the complaint. This is consistent with our established role as an informal alternative to the courts. In considering this complaint I've had regard to the relevant law and regulations; any regulator's rules, guidance and standards, codes of practice, and what I consider was good industry practice at the time.

It's my conclusion that Mrs J authorised these payments. In this context, '*authorised*' essentially means the customer gave the business an instruction to make a payment from their account. In other words, they knew that money was leaving their account, irrespective of where that money actually went.

I appreciate Mrs J says she made the later payments under pressure from the scammers, but that doesn't change the fact that she gave the instructions. I've noted her comments about her mental state at the time, along with the statement from her husband, but without supporting medical evidence, I don't think this is sufficient to show she wasn't capable of understanding what she was doing. Nat West has also confirmed that it wasn't informed at the time that Mrs J was vulnerable in any way, meaning it couldn't take this into account in deciding whether to process the payments it was asked to make.

In broad terms, the starting position at law is that a bank is expected to process payments a customer authorises it to make, in accordance with the Payment Services Regulations and the terms and conditions of their account. There are, however, some situations where we believe a business, taking into account relevant rules, codes and best practice standards, shouldn't have taken its customer's authorisation instruction at 'face value' – or should have looked at the wider circumstances surrounding the transaction before making the payment.

NatWest also has a duty to exercise reasonable skill and care, pay due regard to the interests of its customers and to follow good industry practice to keep customers' accounts safe. This includes identifying vulnerable consumers who may be particularly susceptible to scams and looking out for payments which might indicate the consumer is at risk of financial harm.

Taking these things into account, I need to decide whether NatWest acted fairly and reasonably in its dealings with Mrs J.

The payments

I must take into account that many similar payment instructions NatWest receives will be entirely legitimate and I also need to consider its responsibility to make payments promptly.

Having considered what NatWest knew about payments 1 to 4 at the time, I'm not persuaded it ought to have been particularly concerned. The payments were relatively few in number and low in value, meaning a pattern of multiple, rapid and increasing payments consistent with many known types of scam hadn't yet begun to emerge.

When payments 5 to 8 were made, NatWest knew Mrs J had recently fallen victim to a scam and that payments to cryptocurrency carried a greater risk of being associated with fraud. But on the other hand, they came several weeks after the previous payments and were to a different payee, meaning they weren't obviously linked to the scam she'd reported in July. Further, I don't believe it was necessarily unreasonable for the bank to think Mrs J wouldn't continue making payments to what she appeared to have clearly identified was a scam. In addition, I'm conscious the payments were relatively low in value and were spread out over a period of several weeks, so again I don't think a pattern of payments consistent with many known types of scam had begun to emerge.

On balance and taking everything into account, I don't think there were sufficient grounds for NatWest to suspect Mrs J was at risk of financial harm from fraud when she made these payments and I can't say it was at fault for processing them in line with her instructions and without providing scam warnings or otherwise attempting to intervene.

I want to be clear that it's not my intention to suggest Mrs J is to blame for what happened in any way. She fell victim to a sophisticated scam that was carefully designed to deceive and manipulate its victims. I can understand why she acted in the way she did. But my role is to consider the actions of NatWest and, having done so, I'm not persuaded these were the cause of her losses.

Recovery of funds

Mrs J isn't entitled to a refund under the industry's reimbursement scheme for authorised push payment (APP) fraud. Payments 1 to 7 aren't covered as they were made by card and the scheme doesn't cover card payments. Transfers are covered under the scheme, but not if these are to another account in the customer's own name as is the case with payment 8 here. This notwithstanding, I've looked at whether NatWest could or should have done more to try and recover Mrs J's losses once it was aware that the payments were the result of fraud.

Although Mrs J first reported the scam promptly on 20 July, payments 1 to 4 had already been processed by the bank and it was too late to stop them. The correct method for recovering card payments once they've been processed is the chargeback scheme. This is a voluntary agreement between card providers and card issuers who set the scheme rules and isn't enforced by law. A chargeback isn't guaranteed to result in a refund, there needs to be a right to a chargeback under the scheme rules and under those rules the recipient of the payment can defend a chargeback if it doesn't agree with the request.

I'd only have expected NatWest to raise a chargeback claim if it was likely to be successful and it doesn't appear that would have been the case here. The payments were sent via a legitimate money transfer service that provided the service requested of it, that of collecting money from Mrs J's account and forwarding it on using the account details she provided. Her disagreement is with the scammers, not the money transfer service, and it wouldn't have been possible for NatWest to process a chargeback claim against the scammers as she didn't pay them directly.

Payments 5 to 8 transferred funds to a legitimate cryptocurrency account in Mrs J's own name. From there, she purchased cryptocurrency and moved it onto a wallet address of her choosing (albeit on the scammers' instructions). NatWest could only try to recover funds from her own account and it appears the money had already been moved on by the time the scam was reported. And if hadn't, anything that was left would still have been available to her to access in any event.

In the circumstances, I don't think anything that NatWest could have done differently would likely have led to these payments being successfully recovered.

In conclusion

I recognise Mrs J has been the victim of a cruel scam and I'm sorry she lost this money. I realise the outcome of this complaint will come as a great disappointment but, for the reasons I've explained, I think NatWest acted fairly and reasonably in its dealings with her and I won't be telling it to make any refund.

My final decision

My final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs J to accept or reject my decision before 24 February 2026.

James Biles
Ombudsman