

The complaint

Miss K complains that National Westminster Bank Plc ('NatWest') won't refund the money she lost when she was the victim of a scam.

What happened

Miss K is represented in this case but for ease I'll refer to Miss K throughout my decision.

Miss K says that she saw a story on a messaging app about a celebrity who was endorsing the services of a personal shopper the celebrity had used. The endorsement featured a video of the celebrity receiving goods she had ordered and the personal shopper's profile. Miss K says she contacted the personal shopper and was advised of the process to buy goods and of other celebrities who had used the service.

Miss K placed an order for goods and was advised that the most secure way to pay was via cryptocurrency. I have set out in the table below all the transactions Miss K made to a cryptocurrency account in her own name (with C).

Date	Amount
06/06/23	£2,250
21/06/23	£1,500
21/06/23	£1,500
11/09/23	£50
02/10/23	£100
02/10/23	£200
02/10/23	£1,500
02/10/23	£900
02/10/23	£900
02/10/23	£900
02/10/23	3 x £900 credit
Total	£7,100

The initial payments were for the goods, but Miss K was later advised of fees. Ultimately, she didn't receive the items she had ordered, and Miss K saw on an online forum that others also didn't receive what they had ordered. Miss K reported what had happened to NatWest in October 2023.

NatWest said it acted in accordance with its legal and regulatory requirements and its agents acted professionally and in line with its service standards. NatWest said it couldn't reimburse

Miss K as funds went to an account in her own name, and also noted that it provided her with tailored scam warnings.

Miss K was unhappy with NatWest's response and brought a complaint to this service.

Our investigation so far

The investigator who considered this complaint didn't recommend that it be upheld. He said that the Lending Standards Board's Contingent Reimbursement Model Code (CRM Code) doesn't apply as the payments were made to an account in Miss K's own name, and that NatWest acted reasonably in not intervening when the transactions were made. This was because Miss K made a £1,000 payment to the cryptocurrency account previously, the payments were relatively low in value and were spaced out over a three month period, and the reducing pattern of payments wasn't concerning.

Miss K didn't agree with the investigator's findings, so the complaint has been passed to me to decide. In summary, she said:

- The frequency of cryptocurrency payments was increasing and there were credits to the account which were immediately sent to a cryptocurrency exchange.
- NatWest ought to have been aware of the risks posed by these payments and put measures in place as the Financial Conduct Authority (FCA) and Action Fraud published warnings about cryptocurrency scams in 2018.
- Miss K was vulnerable and under immense stress at the time of the scam as a result of her mother's illness. She was making payments as the scammer advised she would be able to seek private healthcare for her mother (I assume when she sold the items she was purchasing for a profit).

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.

In deciding what's fair and reasonable, I am required to take into account relevant: law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to have been good industry practice at the time.

As the transactions were to an account in Miss K's own name the CRM Code doesn't apply.

It isn't in dispute that Miss K has fallen victim to a cruel scam, or that she authorised the payments to her cryptocurrency wallet (from where that cryptocurrency was subsequently transferred to the scammer).

By June 2023, when these transactions started, banks like NatWest had been aware of the risk of multi-stage scams involving cryptocurrency for some time. The FCA and Action Fraud published warnings about cryptocurrency scams in mid-2018 and scams involving cryptocurrency have increased in prevalence since then. By the end of 2022 many high street banks had taken steps to either limit their customer's ability to purchase cryptocurrency using their bank accounts or to increase friction in relation to cryptocurrency related payments, owing to the elevated risk associated with such transactions.

Taking all of the above into account, I don't think that the fact the payments in this case were going to an account held in Miss K's own name should have led NatWest to believe there wasn't a risk of fraud. I've gone on to consider whether there were factors that ought reasonably to have led NatWest to be concerned that Miss K might be falling victim to a scam.

Miss K's statement shows that she made a payment of £1,000 to C in February 2023, some months before the scam. This means that when she made the scam payments, she wasn't paying a new payee and buying cryptocurrency wasn't entirely out of character. The first

scam transaction Miss K made wasn't for a significantly greater amount and wasn't at the level where I'd expect NatWest to believe it was part of a scam. There is a balance to be struck between protecting customers from fraud and minimising disruption to legitimate payments.

Two weeks after the initial scam transaction Miss K made two consecutive £1,500 payments. I consider it to be arguable that when Miss K made the second payment of £1,500 NatWest ought to have provided a written warning tailored to cryptocurrency investment scams, irrespective of the reason given for the payment (because it was clear the payment was going to a cryptocurrency exchange). But Miss K wasn't investing, she was buying goods and using cryptocurrency as a secure payment method. In the circumstances, I'm not persuaded that a tailored written warning of this nature would have been impactful, or that it would have led to Miss K deciding not to make the payment. I'm not persuaded that NatWest needed to do more than provide such a warning.

Later payments were low in value and the pattern of them wasn't consistent with common investment scams, so I'm not persuaded that NatWest needed to do anything more when they were made. Whilst there was a series of payments on 2 October 2023, the value of each transaction wasn't significant and there wasn't a pattern of increasing payments.

Miss K has referred to the fact she was vulnerable when the transactions were made. I am sorry to hear about the position Miss K was in, but I haven't seen any evidence to suggest that Miss K made NatWest aware or asked for any additional protection to be put in place.

Overall, whilst I'm sorry to hear about Miss K's loss, I can't reasonably ask NatWest to reimburse her.

My final decision

For the reasons stated, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss K to accept or reject my decision before 4 June 2024.

Jay Hadfield
Ombudsman