DRN-5297044

The complaint

Mrs M has complained that National Westminster Bank Plc ("NatWest") failed to protect her from falling victim to a scam, and hasn't refunded all of the money she lost.

What happened

The background of this complaint is already known to both parties, so I won't repeat all of it here. But I'll summarise the key points and then focus on explaining the reason for my decision.

Mrs M has used a professional representative to refer her complaint to this service. For the purposes of my decision, I'll refer directly to Mrs M, but I'd like to reassure Mrs M and her representative that I've considered everything both parties have said.

Between 4 January 2022 and 15 March 2022, Mrs M transferred a total of £10,786.70 from her account held with NatWest. The payments were sent a cryptocurrency platform which I'll call "C" and an individual ("the scammer") who would allegedly facilitate the transfer of funds as part of what Mrs M believed to be an investment. Mrs M says she was introduced to the scammer by an acquaintance, and says she didn't conduct any additional research on the investment as she was shown a certificate authenticating its legitimacy. She's also said she was promised a three-fold return on her investment.

Mrs M has explained that the scammer acted as the introducer to the scam which The Financial Conduct Authority (FCA) has since issued a warning about. Mrs M says that despite her efforts she's been unable to recover any of the money she transferred.

The payments related to this scam were as follows:

	Date	Amount	Description
1	04/01/2022	£1,000	Debit card to crypto platform
2	05/01/2022	£272	Debit card to crypto platform
3	05/01/2022	£1,000	Transfer to L
4	05/01/2022	£1,000	Transfer to L
-	05/01/2022	+£166	Incoming payment from L
5	07/01/2022	£1,042	Transfer to L
6	10/01/2022	£19.72	Transfer to L
7	10/01/2022	£1,042	Transfer to L
8	10/01/2022	£1,260	Transfer to L
9	11/01/2022	£107.98	Debit card to crypto platform
10	10/02/2022	£30	Debit card to crypto platform
11	10/02/2022	£790	Debit card to crypto platform
12	10/02/2022	£25	Debit card to crypto platform
13	10/02/2022	£22	Debit card to crypto platform
14	11/02/2022	£1,040	Transfer to L
15	17/02/2022	£200	Debit card to crypto platform
16	28/02/2022	£411	Transfer to L

17	02/03/2022	£725	Transfer to L
18	15/03/2022	£800	Transfer to L
	Remaining loss	**£10,620.70**	

In order to fund what she believed to be an investment Mrs M made payments in two ways. She used her debit card to fund her account at a legitimate cryptocurrency platform, where she then converted the pounds into cryptocurrency. The cryptocurrency was then forwarded to a wallet directed by the scammer, on the belief that it was funding Mrs M's investment account. Mrs M also made direct bank transfers into the scammer's bank account.

Mrs M says that any warnings she received from NatWest didn't meet the standards required by the Contingent Reimbursement Model ("CRM") Code. She believes the warnings were neither clear nor impactful enough to prevent her from proceeding with the payments. She also considers herself inexperienced in financial matters and argues that NatWest should have recognised her vulnerability and taken additional steps to protect her.

Mrs M is seeking full reimbursement of the money she lost as she believes NatWest failed in its duty to protect her. She has also requested interest on this amount at 8% per annum and an additional £1,000 in compensation for the distress and inconvenience caused.

In its response to Mrs M's complaint NatWest said it acted in accordance with its legal and regulatory obligations by processing the payments as Mrs M instructed. It highlighted that it displayed warnings within its online banking system about common scams and provided information on its website and in branches to help customers protect themselves from fraud.

NatWest also explained that its fraud prevention system didn't flag the payments as suspicious because they didn't match known fraud patterns at the time they were made. It explained that it believed Mrs M's payments were genuine and that there were no grounds to block them or intervene further. It has also noted that Mrs M had to confirm she had read and understood the warning messages before making the payments. It also referred the payments to L to its fraud team for it to consider refunding under the CRM Code, although it doesn't appear it told Mrs M it had done that in its complaint response.

Mrs M remained unhappy so she referred the complaint to this service. In the meantime NatWest's fraud team, refunded £8,339.70 to Mrs M, which it explained was a refund of all of the payments made to recipient L, minus the credit she received from L. NatWest also told us that the refund didn't cover the debit card payments Mrs M made to the cryptocurrency exchange as NatWest said the loss occurred when Mrs M sent the cryptocurrency from there to the scammer, and that debit card payments aren't covered by the CRM Code. It also said that in line with its fraud refund policy, it didn't add interest to the refund it had paid.

Our investigator considered everything and didn't think the complaint should be upheld. He considered the refund NatWest had made according to the CRM Code and said that he thought it was fair. He agreed the debit card payments to the cryptocurrency platform aren't covered by the CRM Code, as the code only covers certain types of payment, and debit card payments aren't one of them. He also didn't think NatWest ought reasonably to have been prompted to intervene before the debit card payments (that constitute Mrs M's outstanding loss) were made, as he said they weren't particularly remarkable when considered in the context of the rest of Mrs M's account usage.

As Mrs M didn't accept the investigator's opinion, the case has been passed to me to make a decision.

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'm not upholding the complaint, broadly for the same reasons as our investigator, which I've explained below.

In broad terms, the starting position is that a firm is expected to process payments and withdrawals that its customer authorises, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. And in this case it's not in question whether Mrs M authorised these payments from leaving her account. It's accepted by all parties that Mrs M gave the instructions to NatWest and NatWest made the payments in line with those instructions, and in line with the terms and conditions of Mrs M's account.

But that doesn't always mean that the business should follow every instruction without asking further questions or intervening to ensure requests coming from their customers are firstly genuine, and secondly won't result in harm.

NatWest has refunded all the payments Mrs M made to L (minus the credit she received) under the CRM Code, which I think is fair. I say this because I haven't been made aware that any of the permitted exceptions apply, and as NatWest has said it believes Mrs M had a reasonable basis to believe the payments were legitimate. NatWest isn't required to pay interest on payments refunded under the CRM Code so I haven't considered them any further, as I'm satisfied Mrs M has been put in the position she'd have been in if she hadn't made them.

Additionally, I'm not aware that Mrs M reported the scam to NatWest until the raised a complaint via her representative in March 2024. So I haven't concluded that NatWest delayed making the refund under the CRM Code, as the refund was made on 17 April 2024, which is reasonable.

I've also noted that Mrs M's representative raised the point that Mrs M's claim was for £9,370, but NatWest has refunded a different amount.

I've carefully reviewed Mrs M's bank statements and I'm satisfied that NatWest has refunded the total of all of the payments made to L – as shown in the table above. In addition, NatWest didn't reduce the refund by the £166 that Mrs M received from L. So I'm satisfied that NatWest acted fairly here and in fact Mrs M received more than she lost to this recipient.

I've gone on to consider the debit card payments to decide whether NatWest should further refund them. Although the bank transfers have already been refunded, I've kept in mind the overall pattern of payments to understand the overall pattern of the scam.

The payments Mrs M made to the cryptocurrency platform were clearly identifiable as such. And by the time they were made, in 2022, the Financial Conduct Authority and other organisations had published several warnings about the risks associated with cryptocurrency that NatWest would've had the opportunity to digest. But that doesn't mean NatWest ought to have treated all cryptocurrency-related transactions as inherently high-risk. I recognise that many cryptocurrency transactions are made legitimately and so although I'd still expect NatWest to have been on the lookout for potential fraud or financial harm to Mrs M, I wouldn't have expected it to treat the transactions differently to others on her account simply on the basis that they were linked to cryptocurrency.

Having considered the pattern and values of the debit card payments to the cryptocurrency platform, I don't think that NatWest ought to have identified that they carried an elevated risk of being fraudulent. I say this because the values of the transactions didn't stand out as particularly unusual when considered in the context of Mrs M's prior account history, for example she made payments of £492.60 in October 2021 and £6,000 in November 2021. As all of the debit card payments were for much smaller amounts, with the largest being for £1,000, I don't find them particularly suspicious in appearance.

I'm mindful that Mrs M made four transactions to the cryptocurrency exchange on 1 February 2022 which I accept may've looked more suspicious than the other payments. But by that time Mrs M had made other payments to the same merchant in the preceding month, and the four payments were all low in value, both individually and combined. So I don't think NatWest should've intervened before allowing them to be made.

It's important to bear in mind that although I've only considered the debit card payments to decide whether NatWest should give Mrs M a further refund, I've kept in mind the overall pattern of payments, including the bank transfers, that the payments were made in between. As there's nothing to link the cryptocurrency debit card payments to the transfers Mrs M made to L, there wasn't an identifiable pattern of fraud, even when looking at all of the scam-related transactions. So, again I don't think NatWest ought to have intervened or uncovered the scam.

Following the investigator's opinion Mrs M's representative raised two additional points; one about Mrs M's vulnerability, as well as a request for additional compensation for distress and inconvenience. I've thought about both points carefully, but I don't consider that NatWest should pay Mrs M anything more in this case.

The primary cause of Mrs M's distress was the scam itself, not a failing by NatWest. Whilst I recognise the significant emotional and financial impact this has had on Mrs M, it was the scammer – not NatWest – who was responsible for deceiving her and ultimately taking her money. NatWest's primary role was to process the payments in accordance with Mrs M's instructions, and I've already found that it was not at fault in doing so.

Mrs M's representative has argued that NatWest should've identified her as vulnerable and taken additional steps to protect her. But being inexperienced in financial matters doesn't automatically mean someone is vulnerable, and certainly not to a degree that the bank ought to have recognised it. I haven't seen any information to suggest Mrs M displayed any signs of vulnerability when making these payments or that she gave NatWest any reason to believe she needed additional safeguarding.

It has also been suggested that NatWest should have intervened earlier, particularly given the involvement of a cryptocurrency exchange. But as I've explained, while cryptocurrency transactions do carry risks, they are also often legitimate, and banks need to strike a balance between protecting customers and allowing them to make payments as they choose. In this case, I've not seen anything that should have prompted the NatWest to do more.

NatWest has already refunded the payments that were made directly to the scammer. That's in line with what I would expect under the CRM Code. But I don't think it would be fair to also require NatWest to compensate Mrs M for distress and inconvenience. The harm she's suffered is a direct result of the scam itself, rather than any failing by the NatWest. So I won't be asking NatWest to make an additional payment.

Recovery of the funds

As the payments to cryptocurrency platform C were made using Mrs M's debit card, the chargeback process is relevant here. In simple terms a chargeback is a mechanism for a consumer, via their card provider, to reclaim money from a retailer's bank when something has gone wrong, provided the transaction meets the eligibility criteria. It's for the card provider to decide whether to raise a chargeback, and it only needs to do so if it has a reasonable prospect of success.

It's also relevant to note that raising a chargeback isn't a legal right, and it's for the debit or credit card provider to decide whether to make a chargeback request to the retailer's bank. The process for managing these claims is determined by a set of rules by the card payment networks and there are no guarantees the card provider will be able to recover the money through the chargeback process.

In order for NatWest to raise a successful chargeback it'd need to provide evidence that the merchant didn't provide the goods or services that Mrs M paid for. So although I understand Mrs M used her debit card to fund her cryptocurrency account and ultimately purchase cryptocurrency, which she sent on to a wallet directed by the scammer, there's no evidence the merchant didn't fulfil its obligation to provide the cryptocurrency that Mrs M paid for. So the dispute doesn't lie between Mrs M and the merchant, but instead Mrs M and the scammer. As there wasn't a reasonable prospect of a chargeback claim being successful, I don't think that was a route that NatWest ought to have pursued.

I'm very sorry that Mrs M has fallen victim to this scam and I do understand that my decision will be disappointing. But for the reasons I've set out above, I don't require NatWest to refund the debit card payments that Mrs M made to the cryptocurrency platform.

My final decision

I don't uphold Mrs M's complaint against National Westminster Bank Plc.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs M to accept or reject my decision before 27 February 2025.

Sam Wade
Ombudsman