DRN-4076720

The complaint

Mrs I complains that National Westminster Bank Plc ("NatWest") won't reimburse money she lost to two investment scams.

What happened

Mrs I was looking for investment opportunities online when she was unable to work following a surgery. She says she felt under pressure to do something and earn money. She joined an online group where people were advising on cryptocurrency investments.

In September 2022, Mrs I made several payments totalling £12,599.60 in connection with two investment opportunities. She says both investments turned out to be a scam.

Investment 1

Mrs I was approached by one of the members of the online group who she says convinced her to send a small amount of money to them to invest on their platform. It isn't clear whether this individual worked for an investment firm or ran their own platform. And details about the platform are also unknown.

Mrs I says she was asked to send £450 to an account in the UK. When she questioned the different name on the account, the individual told her they and their partner used that account in the UK, but they were both based in the US. The individual said transferring the money to the UK account would be cheaper for Mrs I as there wouldn't be a transfer fee. They would transfer the money into their US account and open an account for Mrs I as soon as the funds were received.

Mrs I says that after she made a faster payment from her NatWest account on 6 September, the individual stopped responding to her. She messaged the group and was told she'd probably been scammed.

Investment 2

Another member of the group reached out to Mrs I after she was scammed. She says they were messaging each other for a while and the individual said they wanted to help her. They told Mrs I about a platform "C" they'd been using which she could use and possibly recover what she'd lost. Mrs I says the individual said she could earn up to 3% return per day and get a commission if she referred other people. Mrs I says she registered with $400 and was able to withdraw the first day's interest. (These transactions don't appear on her NatWest bank statement.)

Mrs I was then persuaded to send more money to earn a referral commission of $30,000. She says she registered ten accounts (referrals) and paid in $1,000. Although she'd earned her referral commission, Mrs I was unable to withdraw it due to her 'account access level'. She was told she needed to pay a further $5,000 to unlock the access level, and she could withdraw this amount along with the commission. Mrs I says she sourced this amount by using her business account's overdraft. But she was still unable to make a withdrawal as she

was told the funds received were less than the required amount due to transaction fees. Mrs I says it was at that point she realised she'd been scammed again.

The payments in connection to this scam were made using Mrs I's NatWest debit card. She first sent money to a cryptocurrency exchange to convert it into cryptocurrency, before sending it on to the investment account with C (which unfortunately ended up in the scammer's account).

The following transactions were made from Mrs I's NatWest account in September 2022 –

Transaction Date	Type	Merchant/Payee	Amount
6 September	Faster Payment	"J"	£450.00
6 September	Debit card	Wyre Payments	£179.60
7 September	Debit card	Wyre Payments	£500.00
8 September	Debit card	Transak.com	£1,000.00
11 September	Debit card	Transak.com	£1,000.00
14 September	Debit card	Transak.com	£1,000.00
17 September	Debit card	Transak.com	£500.00
21 September	Debit card	Coinbase.com	£70.00
21 September	Debit card	Transak.com	£200.00
21 September	Debit card	Transak.com	£1,000.00
22 September	Debit card	Transak.com	£600
23 September (9:22 am)	Debit card	Transak.com	£1,000.00
23 September (9:29 am)	Debit card	Transak.com	£1,000.00
23 September (9:37 am)	Debit card	Transak.com	£500.00
23 September (10:13 am)	Debit card	Transak.com	£1,000.00
23 September (11:03 am)	Debit card	Wyre Payments	£500.00
23 September (11:33 am)	Debit card	Wyre Payments	£300.00
23 September (3:35 pm)	Debit card	Transak.com	£1,000.00
23 September (6:21 pm)	Debit card	Coinbase.com	£800.00
		Total payments	£12,599.60
		Total credits	£0
		Total loss	**£12,599.60**

Following the first scam, Mrs I completed a dispute form on NatWest's website for 'services not rendered'. It declined her claim. When she reported the second scam, NatWest declined to offer a refund. It said it believed Mrs I had a reasonable understanding of the risks involved in cryptocurrency investments. In its submission to our service, NatWest said it wasn't the point of loss as the payments went to Mrs I's own crypto wallet.

Our investigator didn't think NatWest was liable for Mrs I's loss. He thought the disputed transactions were spaced out and by the point she'd made several transactions in one day they'd become established beneficiaries. So, they wouldn't have triggered the bank's systems. The investigator also considered NatWest's actions in relation to the recovery of funds after it became aware of the situation. He concluded that chargeback was unlikely to be successful, given the payments went to a crypto exchange who had provided the service as expected (that being the exchange of money into cryptocurrency).

Mrs I didn't agree with the investigator's findings and asked for an ombudsman's decision on the matter.

I issued my provisional decision last month. I said that I intended upholding this complaint, and set out the following reasoning:

Investment 1

Mrs I says she reported that she'd been scammed when she disputed the transaction with NatWest. I've reviewed the information NatWest captured on the dispute form she completed online, and it doesn't make any reference to her being scammed. I've also checked NatWest's website to see if Mrs I would have been presented with an option to select scam while completing the dispute form, and it isn't listed as one of the options. That isn't unsurprising given the form Mrs I completed was for card disputes, which the bank would have relied on for the purposes of considering whether recovery was possible under the chargeback scheme. Mrs I didn't make the payment using her debit card, she sent the money electronically via the faster payment service.

That said, I think NatWest could have made further enquiries when it was clear that Mrs I had reported a dispute about a faster payment through the wrong channel. Certainly, by the point she made a complaint about its decision to decline her claim for both scams, I think NatWest ought to have considered Mrs I's claim using the relevant considerations. In this case, the Lending Standards Board's Contingent Reimbursement Mode (CRM) code applies to the faster payment. I can't see that NatWest considered whether it should have reimbursed her the payment under that code, but I'm satisfied it has had the opportunity to do so.

Our investigator's view was that Mrs I wasn't entitled to be reimbursed under the CRM code as the size of the payment didn't warrant the bank to have provided an effective warning. But the provision of an effective warning (or not being expected to provide one in some situations) is just one of the considerations under the standards that NatWest is expected to meet under the CRM code. The starting principle is that a bank should reimburse a customer who is the victim of an authorised push payment (APP) scam except in limited circumstances (or 'exceptions'). It is for the bank to demonstrate that one or more of the exceptions apply. NatWest hasn't asserted that an exception applies.

I've also not seen anything so far that leads to me think that one or more of the exceptions apply in this case. The exception most relevant here would be whether Mrs I had a reasonable basis for belief that (i) the payee was the person she was expecting to pay, (ii) the payment was for genuine goods or services, and/or (iii) the person with whom she transacted was legitimate. I can see she questioned the different name on the recipient account and was given an explanation which reassured her. And she thought she was dealing with a legitimate person who was going to open an investment account for her.

So, based on the information I've seen so far, I think Mrs I should be reimbursed the full amount of £450 under the CRM code. I also think it would be fair and reasonable for NatWest to pay simple interest at 8% per year to this amount as NatWest ought to have refunded this payment much earlier in accordance with the principles of the code. I consider that interest should be calculated from the date NatWest sent its final response to Mrs I's complaint as I believe that its outcome ought to have taken the CRM code into consideration. The interest should be calculated until the date of settlement.

Investment 2

The payments made in connection to the second scam were all made using a debit card. Therefore, the CRM code doesn't apply. While I find the code doesn't apply here, that code isn't the full extent of the relevant obligations that could apply in cases such as this. In accordance with the law, regulations and good industry practice, a bank has a duty to protect its customers against the risk of fraud and scams so far as is reasonably possible. If, in breach of that duty, a bank fails to act on information which ought reasonably to alert a prudent banker to potential fraud or financial crime, it might be liable for the losses incurred by its customers as a result.

I've considered that the disputed payments were sent to legitimate crypto platforms. I accept that buying cryptocurrency is a legitimate exercise. But both the Financial Conduct Authority (FCA) and Action Fraud had warned of crypto exchange and forex trading scams in 2018. And in May 2019, Action Fraud published further warnings that such scams had tripled in the past year. This type of insight is something that regulated businesses, including NatWest, ought to take notice of.

So, even though Mrs I was transferring funds to a crypto account in her name, NatWest ought to have been on the lookout for unusual and out of character transactions. While the transfers were made to her own wallet, scams involving transfers to crypto accounts were well known to banks by this time and I therefore think that where payments were also out of character, potential losses were foreseeable to the originating bank.

I've considered the operation of Mrs I's account in the year leading up to the disputed payments. I don't consider any of the individual disputed amounts as particularly unusual or suspicious such that they ought to have triggered NatWest's fraud detection system. The largest individual amount that Mrs I sent was £1,000, which in my view wasn't that remarkable based on other transactions on her account. Additionally, I can see a history of payments to some crypto exchanges prior to the transactions Mrs I now disputes. She made five payments to Transak.com only months earlier (two in June and three in August; and two payments were for £1,000). There was also a payment to Coinbase in August. So, on the face of it, these were merchants Mrs I had made payments to before for similar amounts. And she hadn't raised any concerns about those payments.

But, given the increased frequency of transactions on 23 September, I think NatWest ought to have been concerned that there was a possibility that something wasn't right. Within a space of 15 minutes, Mrs I had made three debit card payments totalling £2,500 to the same merchant. Certainly, by the time she authorised the fourth payment (around 35 minutes later) I consider that it would have been reasonable for NatWest to have properly questioned Mrs I before executing her authorised instruction.

Even if she had been sending money to a legitimate crypto platform, it didn't follow that Mrs I's money was safe, or that she wasn't at risk of financial harm due to fraud or a scam. In September 2022, I think NatWest had or ought to have had a good enough understanding of how these scams worked to have been able to identify the risk of harm from fraud. Including, that the customer often first purchases cryptocurrency and moves it on to the fraudster under the assumption that they're moving it into their own wallet or account.

Had NatWest done more and warned Mrs I about cryptocurrency scams, I've no reason to doubt that she would have explained the true purpose of her payment. I can't see that Mrs I had been given a reason to think she had to hide this information from her bank. Neither had she been coached to tell them something different. I'm

satisfied that Mrs I would have looked further into the investment opportunity in general, including whether C was regulated here in the UK or abroad. She could have discovered that it wasn't. Indeed, it's likely that Mrs I would have come across the various warnings about cryptocurrency scams following an intervention from NatWest.

I acknowledge that Mrs I has said she was desperate to make money given her situation. But I'm persuaded that she would have paid attention to warnings from her trusted bank, and that a meaningful intervention would likely have exposed the scam. It follows that I also think it's more likely than not that the intervention would have caused her to stop from going ahead with that fourth payment on 23 September, thereby preventing further losses. I therefore currently find that NatWest is liable for Mrs I's losses from that point.

I've also carefully thought about whether Mrs I is partly to blame for what happened. She doesn't appear to have carried out sufficient independent research into the investment opportunity, or cryptocurrency investments in general to reassure herself that the opportunity as presented to her was genuine. What appears to have started off as a means of recovering £450 that she'd lost to the first scam turned into sending several thousand payments without much due diligence.

Additionally, according to NatWest, Mrs I raised concerns about a payment she made to Coinbase in August 2022 – just the month prior to the disputed transactions. While that payment doesn't form part of this complaint and we've not been told that it was made in relation to the scams the disputed payments relate to, it's reasonable to expect independent research to be carried out to be satisfied that an investment opportunity is genuine where it's clear that there have been previous instances of concern.

I asked Mrs I about the earlier payments to crypto exchanges which haven't been disputed, and I questioned her about her claim that she had no investment experience at all. Mrs I has explained that those payments simply involved converting money into cryptocurrency with the belief that its value would increase over time. There was no cryptocurrency trading involved.

Having given this a lot of thought, I do think that Mrs I ought to bear some responsibility for her losses and that compensation should be reduced accordingly. I intend concluding that it would be fair to reduce compensation payable in relation to the second scam by 20%.

I've also thought about recovery in relation to earlier payments. But like our investigator, I don't think recovery was likely. Although Mrs I was scammed by C, her payments went to legitimate crypto exchanges. NatWest could have only raised a chargeback against the merchant she paid, not another firm. And given the merchant she paid had provided the service (conversion of money into cryptocurrency), a chargeback wouldn't have been successful. So, I don't think NatWest acted unfairly by not raising a chargeback.

I invited further comments from both parties.

Mrs I agrees that she should take some responsibility for her actions. She's said she'd be happy to consider her complaint resolved to her satisfaction if she could be refunded half her loss. Mrs I's asked if this is something I consider reasonable, and whether NatWest would like to mediate.

NatWest accepts my provisional decision. And following our investigator putting forward Mrs I's request, it's said it agrees with the conclusions reached by the ombudsman following an in-depth review of the complaint. And it sees no reason to depart from that.

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 thank both parties for their response to my provisional decision.

I acknowledge that Mrs I considers a 50% refund of the total loss to be a satisfactory resolution to her complaint. But in my provisional decision, I explained why I consider the conclusion I've reached is both fair and reasonable.

To be clear, these were two different scams. It's not that I've found that NatWest ought to have intervened at the time of the first payment (the first scam) and so it follows it should also refund the remaining payments. I've concluded that NatWest should reimburse the first payment under the requirements of the CRM code which it is signed up to. That code doesn't apply to the remaining payments (the second scam). In my provisional decision I explained why I consider NatWest can be held liable for only the last five debit card payments, and why Mrs I should also bear some responsibility in relation to those payments.

In summary, having considered the additional responses I've received from Mrs I and NatWest, I see no reason to depart from the findings I made in my provisional decision.

Putting things right

To put matters right, National Westminster Bank Plc needs to –

- Reimburse Mrs I £450 which she paid in relation to the first scam. NatWest should have reimbursed that payment in line with the CRM code much earlier. But because it didn't, I think it's fair that it adds simple interest at 8% per year on that amount from the date of its final response to the date of settlement.

- Refund the last five debit card payments made on 23 September 2022 (see table above) in relation to the second scam, making a 20% deduction for contributory negligence. I'm not making an interest award in this instance as from what I've seen so far, Mrs I was interested in cryptocurrency investment and so it's reasonable to assume she would have traded on a genuine platform but for the scam. Given the volatility with these types of investments, there's no guarantee that Mrs I would have made a return.

My final decision

For the reasons given, I uphold this complaint and require National Westminster Bank Plc to put things right for Mrs I as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs I to accept or reject my decision before 17 May 2023.

Gagandeep Singh
Ombudsman