DRN-4341893

The complaint

Miss M complains that National Westminster Bank Plc didn't do enough to protect her from the financial harm caused by an investment scam company, or to help her recover the money once she'd reported the scam.

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.

Miss M's cousin's Instagram was hacked by scammers who posted stories on her account about cryptocurrency investments generating large profits. Having seen the posts, Miss M engaged in messages with the account which were from the scammer, pretending to be her cousin.

The scammer recommended a social media page where Miss M she came into contact with an individual claiming to work for a company I'll refer to as "B" who said they could assist her to invest in cryptocurrency. The broker asked her to first purchase cryptocurrency through a cryptocurrency exchange company and then load the cryptocurrency onto her online wallet. Between 15 October 2022 and 17 October 2022, she made six payments to a cryptocurrency exchange company totalling £11,507.91.

To fund the investment, Miss M took out a £4,000 loan with NatWest. And when she needed money for what she understood was a withdrawal fee, she tried to borrow money from her brother who researched the investment and told her it could be a scam.

Miss M complained to NatWest, but it said it wouldn't refund the money she'd lost. It said it wasn't the point of loss and it had acted on her genuine instructions to make the payments and Miss M had failed to carry out due diligence. It explained it's required to make payments in accordance with the instructions of its customers and it can only deviate from this position where it has reasonable grounds to suspect that a payment would result in a customer being the victim of a fraud.

It said it places appropriate and relevant warning messages across its online banking facility to warn customers about scams, and the information is available on its websites and within its branches. Warning messages are displayed to consumers before making payments, and tailored warnings are displayed before making a transfer or adding a new payee.

It explained the disputed payments were made by Miss M using her secure online banking facility, so there were no concerns, they didn't match any fraud trends and were not deemed suspicious, so a security check was not generated.

Miss M wasn't satisfied and so she complained to this service, arguing NatWest should refund the payments and write off the loan. Her representative said the account behaviour was concerning because it was much more than she'd even spent and should have triggered an intervention. They said that if NatWest had intervened, Miss M would have told it she

came across an investment on social media, and it would immediately have identified this as a known fraud trend targeted at young people.

It said Miss M sent a text message on 15 October 2022 to confirm the payment was genuine and there was no reason given for the loan. It maintained it had acted on Miss M's genuine instruction to make the payments, the debit card payments weren't covered by the Contingent Reimbursement Model (CRM) code and there was no prospect of a successful chargeback because the merchant had fulfilled their services.

It said the payments weren't flagged as unusual or suspicious and Miss M had confirmed via text message that the payment was genuine. It also said the fact Miss M saw the opportunity on social media demonstrates that she was actively looking for an investment opportunity and was not approached or cold called. It pointed out Miss M had said she was promised high returns on the investment and encouraged to invest more to receive greater profits, arguing there were sufficient red flags for her to have questioned whether the investment was genuine.

Our investigator didn't think the complaint should be upheld because she didn't think there was anything NatWest could have done to change the outcome. She explained NatWest is expected to have measures in place to detect unusual activity and intervene appropriately. But she didn't think the payments were particularly unusual or suspicious, so she didn't think it missed an opportunity to identify the scam. She also said there was no prospect of a successful chargeback because its most likely the cryptocurrency exchange company provided the intended service.

Miss M has asked for the complaint to be reviewed by an Ombudsman. She thinks the payments were suspicious, particularly those on 17 October 2022, which totalled £6,000, which exceeds the £5,000 threshold which this service considers suspicious. She says her monthly income is £1,100 and she only uses the account for day-to-day spending.

Her representative argues that NatWest should have realised Miss M was borrowing money to fund an investment and this should have been a red flag, as was the change in account activity. They maintain that if NatWest had intervened, Miss M would have told it she came across the investment on social media and it would have identified this had the hallmarks of a scam and taken steps to warn her that Miss M was at risk of financial harm due to fraud.

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 conclusion as our investigator. And for largely the same reasons. I'm sorry to hear that Miss M has been the victim of a cruel scam. I know she feels strongly about this complaint and this will come as a disappointment to her, so I'll explain why.

I'm satisfied Miss M 'authorised' the payments for the purposes of the of the Payment Services Regulations 2017 ('the Regulations'), in force at the time. So, although she didn't intend the money to go to scammers, under the Regulations, and under the terms and conditions of his bank account, she is presumed liable for the loss in the first instance.

Not every complaint referred to us and categorised as an investment scam is in fact a scam. Some cases simply involve high-risk unregulated investments that resulted in disappointing returns or losses. Some of these investments may have been promoted using sales methods that were arguably unethical and/or misleading. However, while customers who lost out may

understandably regard such acts or omissions as fraudulent, they do not necessarily meet the high legal threshold or burden of proof for fraud, i.e. dishonestly making a false representation and/or failing to disclose information with the intention of making a gain for himself or of causing loss to another or exposing another to the risk of loss (Fraud Act 2006).

I've carefully considered the circumstances, and I am persuaded the broker was operating as part of a scam. But, although Miss M didn't intend her money to go to scammers, she did authorise the disputed payments. NatWest is expected to process payments and withdrawals that a customer authorises it to make, but where the customer has been the victim of a scam, it may sometimes be fair and reasonable for the bank to reimburse them even though they authorised the payment.

Prevention

I've thought about whether NatWest could have done more to prevent the scam from occurring altogether. Buying cryptocurrency is a legitimate activity and from the evidence I've seen, the payments were made to a genuine cryptocurrency exchange company. However, NatWest had an obligation to be alert to fraud and scams and these payments were part of a wider scam, so I need to consider whether it ought to have intervened to warn Miss M when she tried to make the payments. If there are unusual or suspicious payments on an account, I'd expect NatWest to intervene with a view to protecting Miss M from financial harm.

The payments didn't flag as suspicious on NatWest's systems. I've considered the nature of the payments in the context of whether they were unusual or uncharacteristic of how she normally ran her account, and I don't think they were. All the payments were to a legitimate cryptocurrency exchange company and none of them were for particularly large amounts.

Miss M feels the third payment she made on 19 October 2022 should have triggered an intervention because the cumulative sum she paid that day was unusual when compared with the usual spending on her account. She paid £3884.63 on 18 October 2022 and £524.95 on 19 October, so I don't think the amount transferred on 18 October 2022 was high enough to have triggered an intervention. And even if the three transactions had occurred on the same day, by the time she made the final payment, she'd transferred money to the payee on five previous occasions, so it wasn't unusual. So, I don't think NatWest missed an opportunity to intervene.

Chargeback

I've thought about whether NatWest could have done more to recover Miss M's payments when she reported the scam to it. Chargeback is a voluntary scheme run by Visa whereby it will ultimately arbitrate on a dispute between the merchant and customer if it cannot be resolved between them after two 'presentments'. Such arbitration is subject to the rules of the scheme — so there are limited grounds on which a chargeback can succeed. Our role in such cases is not to second-guess Visa's arbitration decision or scheme rules, but to determine whether the regulated card issuer (i.e. NatWest) acted fairly and reasonably when presenting (or choosing not to present) a chargeback on behalf of its cardholder (Miss M).

Miss M's own testimony supports that she used cryptocurrency exchanges to facilitate the transfers to B. Its only possible to make a chargeback claim to the merchant that received the disputed payments. It's most likely that the cryptocurrency exchanges would have been able to evidence they'd done what was asked of them. That is, in exchange for Miss M's payments, they converted and sent an amount of cryptocurrency to the wallet address provided. So, any chargeback was destined fail, therefore I'm satisfied that NatWest's decision not to raise a chargeback request against either of the cryptocurrency exchange companies was fair.

Overall, I'm satisfied NatWest took the correct steps prior to the funds being released – as well as the steps it took after being notified of the potential fraud. I'm sorry to hear Miss M has lost money and the effect this has had on her. But for the reasons I've explained, I don't think NatWest is to blame for this and so I can't fairly tell it to do anything further to resolve this complaint.

My final decision

For the reasons I've outlined above, my final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss M to accept or reject my decision before 19 October 2023.

Carolyn Bonnell
Ombudsman