DRN-4669125

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, or to help her recover the money once she'd reported the scam to it.

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 was the victim of an investment scam and three separate recovery scams.

Scam 1

In September 2021 Miss M came across an advert on social media for an investment company I'll refer to as "S". She clicked on a link to S's website and could see it was based overseas in a country she knew to be a well-renowned financial hub. She called the number on the website and spoke to someone I'll refer to as "the scammer" who said she could start with a small investment. She was asked to provide a copy of her ID, account number and sort code before being contacted by someone who I'll refer to as "the scammer".

The scammer told Miss M he'd place trades on her behalf and asked her to first purchase cryptocurrency through two cryptocurrency exchange companies I'll refer to as "C" and "SB" before loading it onto an online wallet. Between 16 September 2021 and 14 October 2021, she made four payments to C using a debit card connected to her NatWest account and two transfers to SB payments totalling £7,552.80. She also made payments to the scam from other of her accounts and during this period she received four credits from C totalling £196.

In October 2021 Miss M stopped receiving daily updates from the scammer and was unable to access her trading account. When she finally contacted the scammer he said she'd been unable to log in because S was rebranding, but her insurance policy was still in place and there was no change to her agreement with S.

In January 2022, she was told she'd been transferred to a different broker and that S was taking part in the launch of a brand new investment platform. This made Miss M suspicious and so she decided to withdraw her profits. The scammer told her she'd need to pay a fee, so between January 2022 and February 2022, she made a series of transactions from her other bank accounts, eventually realising she'd been scammed when S's website disappeared and she was unable to reach the scammer.

Scam 2

After discovering she'd been scammed, Miss M searched online for recovery companies and sent emails to various companies. She was contacted by someone who said he was an independent fraud investigator and that he would be able to track the lost funds using special software. He asked Miss M to pay for the software and on 1 March 2022, 2 March 2022 and 3 March 2022 she made transfers of £415, £395 and £255 to a cryptocurrency exchange I'll

refer to as “N”. Unfortunately, shortly after she made the payments, the scammer stopped replying, at which point she realised she’d been scammed.

On 27 April 2022, she contacted NatWest to report that she’d fallen victim to a scam, but she was told it wasn’t the point of loss and she should contact the cryptocurrency exchanges she’d paid.

Scam 3

In June 2022 Miss M was contacted by someone I’ll refer to as “the scammer” who introduced himself as a ‘crypto detective’. He said he’d be able to locate the funds and knew how much she’d invested and the profit she’d made. He said she wouldn’t need to make any payments in advance and that he’d take commission once he had recovered her funds.

The scammer told Miss M the funds were locked in a cryptocurrency wallet linked to S and that they could only issue a refund once her cryptocurrency wallet was activated, which was necessary to receive the refund. He told her to download ‘AnyDesk’ so he could guide her to make payments between the two cryptocurrency wallets.

Between 20 June 2022 to 21 June 2022, Miss M made a series of transfers totalling £3,030 to a cryptocurrency merchant I’ll refer to as “R”. But when she transferred the funds between the wallets, they disappeared and she realised she’d been scammed.

Scam 4

On 9 March 2022, Miss M received an email from someone who claimed to work for a recovery company I’ll refer to as “B”. The scammer said she wouldn’t have to pay any fees in advance, and Miss M went ahead because she thought she had nothing to lose.

After a week, the scammer told Miss M he’d recovered the funds and they would be sent to her wallet in the next few days. When she didn’t receive the funds she was told the cryptocurrency platform had blocked the payments so they would instead use a transfer company. The scammer told her she’d have to pay transfer fees and administrative fees and when she still didn’t receive the funds he suggested it could transfer the funds via “Bank R”.

When she still didn’t receive any funds, Miss M made further payments towards what she believed was legal action against Bank R. These payments continued until August 2022 when she realised that this was, unfortunately, an elaborate scam.

The complaint

Miss M complained to NatWest but it refused to refund any of the money she’d lost. It apologised that he had to chase it to find out the outcome of its investigation. But it said she should contact the financial organisations she’d sent the funds to as it couldn’t be considered as the point of the loss. It said it had acted on her genuine instructions to process the payments, she failed to carry out due diligence and didn’t take appropriate care when using a cryptocurrency wallet.

It said it places appropriate and relevant warning messages across its online banking facility to warn customers about scams and information is available on its websites and within its branches. Warning messages are displayed before making a transfer or adding a new payee. A tailored scam warning is also displayed and customers must confirm they are confident they have read and understood the advice and they are satisfied they have taken relevant steps.

It said there were no concerns at that time around the validity of the payments, there would be no recourse as the payments successfully reached the wallet before being withdrawn and the Contingent Reimbursement Model ("CRM") code didn't apply because Miss M had paid accounts in her own name.

Miss M wasn't satisfied and so she complained to this service with the assistance of a representative. She accepted NatWest had contacted her before some of the payments she'd made to the fourth scam but said she wasn't given an effective warning. She argued that it had multiple opportunities to intervene as the payments were unusual and if it had questioned her thoroughly, it would have been apparent to the that she was falling victim to a recovery scam.

Her representative said NatWest should have intervened as Miss M made 44 payments to multiple payees, some of them linked to cryptocurrency. It said there were multiple red flags including the rapid depletion of funds, multiple high payments, a sudden increase in spending, a sudden change to operation of the account and multiple payments made on the same day to the same payee.

They said Miss M normally used the account for daily spending, direct debits payments and transactions between her own accounts and prior to the scam she had never made transactions to payees linked to cryptocurrency. They argued the payment she made on 1 October 2021 for £3,700 was unusual as it was a high value payment to an account linked with cryptocurrency.

They further argued the payments Miss M made between 1 March 2022 and 3 March 2022 2022 were unusual and if it had intervened it would have been obvious she was falling victim to a recovery scam. And the transactions on 21 June 2022 should have been concerning as by this time Miss M had told NatWest she'd been the victim of a scam and the cumulative total of the two payments was £3,000 and she was paying a merchant linked to cryptocurrency. They also said the payments on 7 July 2022 totalling £4,405 should have raised concerns because of the high value of payments made in a single day.

Miss M's representative said she didn't receive any effective pop-up or warning messages and that NatWest should have contacted her to ask questions around when she was making the payments, whether there was a third party involved, how she found out about the company, whether she'd researched the company, whether she'd checked the Financial Conduct Authority ("FCA"), whether she'd been promised unrealistic returns, whether she'd made any withdrawals and whether she'd discussed the investment with anyone. And as she hadn't been prompted to give false answers, she would have told it she was being assisted by a third party and it would have identified that she was being scammed and provided a scam warning.

The representative said that if NatWest had asked Miss M to request a withdrawal during the first scam, it would have been obvious that S wasn't a legitimate investment company and if it had asked why she was making the later payments it would have been obvious she was falling victim to a recovery scam.

NatWest maintained it wasn't the point of loss, the payments were made over a period of a year, they were mostly low value and they were made to numerous payees, so it didn't accept it missed opportunities to intervene. It also said she would have been presented with warning messages before she made the online payments.

Our investigator didn't think the payments were particularly unusual or suspicious considering the normal activity on the account. He considered the statements dating back to

February 2021 and noted Miss M had made transactions of similar amounts, for example £700 on 22 February 2021, £500 on 7 April 2021, £1,000 on 14 April 2021 and 17 August 2021, £1,200 on 15 September 2021 and £2,043.23 on 22 September 2021. There were also sufficient funds in the account to facilitate the payments.

He noted Miss M made four payments on 16 September 2021, but they were low value and in line with the previous account activity, so he didn't think NatWest needed to intervene. He accepted payments five and six were higher in value but he wasn't persuaded this was enough for NatWest to have intervened, especially as she had made a payment of £2,043.23 on 22 September 2021.

He didn't think the payments made to the second scam were unusual they were low value and in line with the normal spending on the account. He noted Miss M made three payments to the third scam on 20 June 2021, but they only totalled £30 and wouldn't have raised any concerns. And she made two further payments the following day totalling £3,000, but there would have been no cause for concern as she'd previously made similar payments.

He explained the payments Miss M made to scam four were spread out and any payments made on the same day were low value, so they wouldn't have been concerning, particularly as it wasn't unusual for her to make multiple payments. He noted the payments were spread out over a four-month period to an established beneficiary and wouldn't indicate a sudden increase in spending. So, he didn't think NatWest missed an opportunity to intervene.

He explained Miss M didn't speak to or interact with NatWest at the time of the payments so he didn't think it missed an opportunity to identify the payments were being made in relation to a scam. And the CRM code doesn't apply to card payments and international payments or to payments to an account in the same name.

Finally, he was satisfied that once NatWest knew about the scam, it reached out to the beneficiary banks but no funds remained and as the main cause for the upset was the scammers who persuaded Miss M to part with her funds and he hadn't found any errors or delays to NatWest's investigation, he didn't think she was entitled to any compensation.

Miss M has asked for the complaint to be reviewed by an Ombudsman. Her representative has argued the value of the payments in the first scam should have raised concerns. And even though she had previously made multiple payments in one day, the frequency of payments to a cryptocurrency platform meant there was a clear scam pattern emerging.

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.

The Contingent Reimbursement Model ("CRM") Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Miss M says she's fallen victim to, in all but a limited number of circumstances. NatWest has said the CRM code didn't apply in this case because Miss M was paying accounts in her own name and I'm satisfied that's fair.

I've thought about whether NatWest could have done more to recover the card 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 payments. 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.

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 her bank account, Miss M is presumed liable for the loss in the first instance.

There's no dispute that this was 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 genuine cryptocurrency exchange companies. However, NatWest ought to fairly and reasonably 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 it to intervene with a view to protecting her from financial harm due to fraud.

The payments didn't flag as suspicious on NatWest's systems. All the payments were to legitimate cryptocurrency exchange companies and there would have been no reason for NatWest to query the first four payments. However, when she made the fifth payment, she was paying a new payee and £3,700 was much more than she'd previously spent on the account. However, it's not unusual for consumers to make higher payments from time to time and the amount wasn't so high that we would expect NatWest to have intervened based on the amount alone.

I've thought about whether the fact Miss M reported the first two scams to NatWest on 27 April 2022 means it ought to have intervened in the payments that followed, but I don't think it does because whether or not a consumer has previously been the victim of a scam, we would only expect NatWest to intervene if there are unusual or suspicious payments on an account.

The next payment event of note were the two payments Miss M made to 21 June 2021, when the cumulative total of both payments was £3,000. But this was the third time since October 2021 that Miss M had paid out £3,000 to a cryptocurrency merchant and so the amount wasn't unusual.

Similarly, by the time she paid £4,405 to C on 7 July 2022 and £5050 on 1 August 2022, the payment amounts had been steadily increasing. She'd been making payments to cryptocurrency merchants for just over a year so by the time she paid £5,050 on July 2022, C was an established payee and she had a history of making multiple payments in one day. So I don't think NatWest needed to intervene.

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.

Recovery

I'm satisfied there wasn't a realistic prospect of a successful recovery because Miss M had paid accounts in her own name and the funds were moved on from there.

Compensation

The main cause for the upset was the scammers who persuaded Miss M to part with her funds and as I haven't found any errors or delays to NatWest's investigation, I don't think she is entitled to any compensation.

My final decision

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 8 April 2024.

Carolyn Bonnell
Ombudsman