DRN-4337070

The complaint

Ms O 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.

In April 2021, Ms O came across an advert about cryptocurrency while she was searching online for investment opportunities. She responded by uploading her contact details and shortly afterwards she was contacted by someone claiming to be a broker working for a company I'll refer to as "W". The broker told her he traded in foreign currency or "forex" and cryptocurrency.

Before going ahead with the investment, Ms O conducted an online search on W, which satisfied her it was a legitimate cryptocurrency exchange platform. She also asked to speak with a senior staff member, who also reassured her the investment was genuine.

The broker asked her to first purchase cryptocurrency through a cryptocurrency exchange company and then load the cryptocurrency onto her online wallet. He told her about another leading cryptocurrency exchange platform and said it would be sensible to use multiple platforms to diversify her portfolio and to avoid any payments being delayed. Between 21 August 2021 and 15 October 2021, Ms O made seven payments to two cryptocurrency exchange companies totalling £29,236.65 via online transfer from her NatWest account.

In December 2021, the broker told Ms O that her investment had increased in value to approximately £150,000, so she tried to make a withdrawal. She realised she'd been the victim of a scam when she was unable to access the funds.

Ms O complained to NatWest, but it refused to refund the money she'd lost. It said that during a call on 21 August 2021, she was asked whether she'd been approached by a broker, and she said she had not. It said she was given several warnings about the risks associated with the investment, including the use of Anydesk software. It also said she was offered additional time to consider the advice, but she declined and insisted it should release the payments.

Ms O wasn't satisfied and so she complained to this service arguing NatWest didn't do enough to identify the transactions as being potentially fraudulent.

NatWest said Ms O had admitted to not having read the online warning messages displayed prior to making the disputed transfers, and during the call on 21 August 2021 she said several times that she hadn't been approached by a broker. And she ignored the warnings it gave about the potential risks. It also said she took six months to report the scam, and that the payments of £273.36 and £1,903.63 on 3 September 2021 and 23 October 2021 were

credits into her account from the cryptocurrency exchange, not payments out as she'd originally claimed.

NatWest also said a further payment had flagged for checks on 26 August 2021 when Ms O tried to transfer £4,500. It was unable to provide a recording, but it said Ms O confirmed the payment was genuine and a scam warning was provided.

Our investigator didn't think the complaint should be upheld. She explained the Contingent Reimbursement model ("CRM") code didn't apply to the payments because they were to an account in Ms O's name and control. She noted Ms O disputed the account was in her name and control, but she hadn't provided any evidence to support this.

Our investigator said NatWest should have done more during the call on 21 August 2021 because there were hallmarks present including the use of AnyDesk and the fact this was a payment to a cryptocurrency exchange. She thought NatWest should have asked questions about whether the money would be transferred on from the cryptocurrency exchange, how she came across the investment opportunity and whether she received any documentation from the merchant confirming her investment. But she didn't think this would have made any difference to the outcome because she didn't think Ms O would've been forthcoming or truthful in her responses to further questions.

She didn't think NatWest ought to have intervened when Ms O made the later payments because by then there was an established pattern of spending, so the payments weren't unusual and given the time that had elapsed, it was unlikely it would have been able to recover the funds from the recipient account.

Ms O has asked for her complaint to be reviewed by an Ombudsman. Her representative has explained Ms O built a strong, trusting relationship with the broker and he took advantage of her lack of investment experience. They explained they would talk almost every day and he portrayed himself as very confident and knowledgeable and that he had her best interests in mind.

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 Ms O 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 CRM Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Ms O says she's fallen victim to, in all but a limited number of circumstances. NatWest said the CRM code didn't apply in this case because the disputed payments were paid to an account in Ms O's name, and I'm satisfied that's fair.

Her representative has suggested that Ms O didn't consider the cryptocurrency exchange account was in her name and control because it was set up during the course of fraud, but she told NatWest the account was in her name during the call on 21 August 2022 and in the absence of any evidence to the contrary, I'm satisfied that was the case and that the wallet addresses she says were provided by the broker were not the accounts she paid money to from her NatWest account.

I'm also satisfied Ms O '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, Ms O 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 Ms O 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 had an obligation to be alert to fraud and these payments were part of a wider scam, so I need to consider whether it ought to have done more to warn Ms O 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 Ms O from financial harm due to fraud.

The first payment did flag as suspicious on NatWest's systems, and I've listened to the call dated 21 August 2022, during which Ms O confirmed the payment was genuine and that she hadn't been instructed to move the money by a third party. She said the cryptocurrency exchange account was in her control and that she hadn't been contacted by anyone claiming to be an account manager or broker. There was also a conversation about Anydesk and she told the call handler her friend had told her to download it because he was helping her with a problem with her computer.

The call handler checked she hadn't given anyone access to the account she held with the cryptocurrency exchange company, and she confirmed that she hadn't. He also asked whether she'd researched the investment and that she understood the risks, including the fact the payee wasn't regulated by the Financial Conduct Authority ("FCA"). She was then read a scam warning from the FCA website before the payment was released.

Unfortunately, Ms O wasn't entirely open in her responses, and this meant the call handler didn't have enough information to identify this was a scam. Our investigator has said he should have asked more questions about whether she planned to transfer the money on from the cryptocurrency exchange, how she learned about the investment opportunity and whether she had received any documentation from the merchant to confirm her investment.

Considering her responses and the fact this was a large payment I think the call handler probably did enough. But I agree with our investigator that even if the call handler had been more robust in his questions, it's unlikely she'd have divulged any more information and so it

wouldn't have made any difference to the outcome, especially as she'd done some research and built a rapport with the broker.

So, in the absence of any warnings on either the FCA or IOSCO websites, having pointed out the fact Anydesk was associated with scams and providing a warning about the risk of scams, there was little else NatWest could reasonably have done to change Ms O's mind about going ahead with the investment.

The payments increased in value as the scam progressed. But NatWest intervened again on 26 August 2021 and so by 30 September 2021 when she paid £6719.13 to the second cryptocurrency exchange, there was an established pattern of spending and there had been two calls during which Ms O had been given scam warnings. So, the later payments weren't unusual or suspicious and there was no reason for NatWest to intervene again.

Overall, I'm satisfied NatWest took the correct steps prior to the funds being released – as well as the steps they took after being notified of the potential fraud. I'm sorry to hear Ms O 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 Ms O to accept or reject my decision before 1 November 2023.

Carolyn Bonnell
Ombudsman