DRN-4316124

The complaint

Mr R complains that National Westminster Bank Plc didn't do enough to protect him from the financial harm caused by an investment scam company, or to help him recover the money once he'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.

Mr R was invited to join a telegram group which was run by someone claiming to be affiliated with a financial website. The broker advised the group to invest in cryptocurrency using a platform I'll refer to as "G", describing the investment as "a top-notch new energy finance product that combines the four innovative technologies of Natural Gas + Web 3.0 + Blockchain + Metaverse".

Mr R was sent a 'white paper' which outlined the investment opportunity and after careful consideration he decided to invest. Between 23 November 2022 and 5 March 2023, Mr R made thirteen payments from his NatWest account to an account he held with a cryptocurrency exchange company totalling £121,401. The funds were then moved to an online wallet which he could monitor on G's trading platform.

When Mr R tried to check on his investment, he found it had been deleted, that G's platform was no longer available and all the chat history on the telegram group had been deleted. At this point he realised he was the victim of an investment scam and complained to NatWest. NatWest said there was nothing it could do because it wasn't the point of loss. It also said the Contingent Reimbursement Model ("CRM") code wouldn't apply to the payments because they were to an account in Mr R's name, so they weren't covered by the code.

It said Mr R had made the payments using its secure online banking facility and there were no concerns at that time on the validity of the payments. It also said the payments weren't unusual and didn't alert because they were genuine transactions made using Mr R's secure online banking.

NatWest also explained it places appropriate and relevant warning messages across its online banking facility to warn customers about scams and before making a payment, and that a message is also displayed on its online banking facility.

Mr R's representative said the new and large transactions to a high-risk cryptocurrency merchant was a huge change of behaviour on the account. They said the maximum payment he'd made previously was £10,000, yet the first of the disputed payments was £15,000, which was significantly larger than the previous largest investment.

They said NatWest should have questioned the payment as it was out of character and if it had intervened and asked questions around the purpose and circumstances of the payment, it would have been able to spot it had the red flags of a common cryptocurrency scam. They said the red flags included the fact Mr R was contacted on social media regarding the

investment, he was told the returns would be over 100% and he was told he'd have to pay a large amount of tax to make a withdrawal.

NatWest said it was unable to raise a chargeback request for the disputed debit card payments as the merchant had fulfilled their services. It also said Mr R would have been given a warning message urging him to check the transaction was genuine, and by acknowledging the warning message, he confirmed he was happy to proceed.

NatWest also questioned whether Mr R had done adequate due diligence and maintained the payments weren't flagged because he'd previously made large payment from his account. And it said it was unable to recover the funds as the payments were sent to Mr R's own wallet account.

Our investigator didn't think the complaint should be upheld stating Mr R had previously made larger payments, so she didn't expect NatWest to have flagged the payments. She said Mr R had made several large transactions, for example £8,361, £50,000, and £50,000 on 31 January 2022, £49,000 on 31 March 2022, £42,000 on 1 April 2022, £9,972.01 on 14 April 2022, two payments of £10,000 on 3 May 2022, £8,000 on 6 May 2022, £5,000 on 28 October 2022 and 10,003.12 on 1 November 2022. There was also £23,497.53 paid into the account on 26 April 2022, £14,991 on 18 May 2022, £41,845.04 on 13 July 2022.

She didn't think the disputed payments were out of character when compared with the usual spending on the account, so she didn't think NatWest needed to intervene. And she said the CRM code didn't apply as funds were transferred into Mr R's own cryptocurrency account and included card payments.

Mr R has asked for the complaint to be reviewed by an Ombudsman arguing that even though there were large payments from the account, the disputed payments should have stood out because they were to new payees and related to cryptocurrency. He pointed out the previous payments were to HMRC, existing payees or UK based accounts. He accepted the £5,000 payment on 28 October 2022 did relate to an investment, but it explained it didn't relate to cryptocurrency and was considerably less than £15,000.

The representative argued the first payment was a payment to a cryptocurrency exchange which was larger than any previous transfer to a new payee, and Mr R was able to send £27,000 and £21,000 without any intervention. They said the other large payments were to existing payees for ISA's or to HMRC, so they were an entirely different profile to the disputed payments, so the disputed payments were unusual and should have triggered an intervention.

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 Mr R has been the victim of a cruel scam. I know he feels strongly about this complaint, and this will come as a disappointment to him, 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 Mr R says they've fallen victim to, in all but a limited number of circumstances. The CRM code didn't apply in this case because the payments were to an account in Mr R's own name.

I'm satisfied Mr R 'authorised' the payments for the purposes of the of the Payment Services Regulations 2017 ('the Regulations'), in force at the time. So, although he didn't intend the money to go to scammers, under the Regulations, and under the terms and conditions of his bank account, Mr R 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 Mr R didn't intend his money to go to scammers, he 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 Mr R when he 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 Mr R from financial harm due to fraud.

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 Mr R normally ran his account, and I don't think they were. All the payments were to a legitimate cryptocurrency exchange company and, while I accept they were for large amounts, this wasn't unusual when compared to the usual spending on the account. Our investigator has explained that between 31 January 2022 and 1 November 2022, Mr R had made several large payments from the account, including three payments totalling £108,361 on 31 January 2022 and £10,003.12 on 1 November 20221, which was only 22 days before the first of the disputed payments. There were also several large payments into the account.

Mr R and his representative have said these payments can't be compared to the disputed payments because they included payments to HMRC, and ISA payments, which were existing payees. I accept the first of the disputed payments was to a new payee, but the cryptocurrency exchange company was a legitimate company and I'm not persuaded the fact he hadn't made a payment to that particular company before constitutes enough of a distinction to the other high value payments to mean NatWest should have intervened, especially as the £5,000 payment on 28 October 2022 related to investments.

Finally, I accept that Mr R went on to make payments for £21,000 on 2 March 2022 and £27,000 on 5 March 2022 but by this time, there was an established pattern of spending to a payee he'd paid many times before and so there was no reason for NatWest to have intervened at that point.

Chargeback

I've thought about whether NatWest could have done more to recover Mr R's payments when he 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 (Mr R).

Mr R's own testimony supports that he used cryptocurrency exchanges to facilitate the transfers. Its only possible to make a chargeback claim to the merchant that received the disputed payments. It's most likely that the cryptocurrency exchange would have been able to evidence they'd done what was asked of them. That is, in exchange for Mr R'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 the cryptocurrency exchange company was fair.

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 Mr R has lost money and the effect this has had on him. 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 Mr R to accept or reject my decision before 23 October 2023.

Carolyn Bonnell
Ombudsman