DRN-4420677

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 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.

In May 2022 Mr R received a phone call from someone who I'll refer to as "the scammer" who claimed to work for company "P". He told Mr R he had £160,000 left in bitcoin from an investment he'd made several years ago, and they had managed to trace the funds back to him. The scammer knew how much Mr R had invested and he believed what he was told because he had previously invested in cryptocurrency and had been unable to access his profits.

Mr R looked on P's website, which looked extremely professional and featured functions such as live quotes, market, and pending orders as well as different charts and graphs. P also had a London address and several contact numbers and email addresses. He confirmed he wanted to go ahead and was allocated a senior financial advisor who sent a letter of guarantee confirming he would be able to withdraw the funds once he'd proven his liquidity. He was also told he would be assigned a money laundering reporting officer to assist him during the process of releasing the cryptocurrency from Blockchain to his bank account.

The advisor asked Mr R to download Team Viewer, explaining they needed a record of the transfers to prove the deposits were being made correctly. He also instructed him to open accounts with two Electronic Money Institutions I'll refer to as ("R") and ("W") as this would make the transfers easier. And he advised him to first purchase cryptocurrency through a cryptocurrency exchange company and then load the cryptocurrency onto an online wallet.

Between 6 June 2022 and 9 September 2022, Mr R made thirteen payments from his NatWest account to W totalling £116,518.30. On 6 June 2022, he transferred £2,000, £10,000 and £8,000 from his NatWest account. It intervened twice on 6 June 2022 and the payments were released. But he tried to pay a further £20,000 on 7 June 2022 and this payment was blocked. During the calls that followed, Mr R told NatWest he was lending money to a friend in Portugal for mortgage fees and medical expenses, and the fraud team refused to release the payment on the basis it could be a scam.

Mr R's account was blocked for a period until 29 July 2022 when he made two payments of £1,005 and £18,900. On 1 August 2022 he made a further payment of £20,000 which was blocked by NatWest. During the call he told it the purpose of the payments and was warned it could be a scam, but he confirmed he wanted to go ahead. He went on to make a further four payments and realised he'd been scammed when was told his investment had risen to £773,899.79 and he would have to pay 25% of this sum for the funds to be released.

Mr R complained to NatWest arguing it had failed to identify the payments were unusual or provide adequate scam education. NatWest said it had acted on Mr R's instructions to make the payments, he had failed to carry out due diligence and it wasn't the point of loss, so it was unable to assist. It said it places appropriate and relevant warning messages across its online banking facility and before making a payment or adding a new payee, a message is displayed to warn customers about the types of scams it sees.

It also said the payments were made to accounts in Mr R's own name, so it was unable to recover funds as it wasn't the point of the loss, and they weren't covered under the Contingent Reimbursement Model ("CRM") code.

Mr R wasn't satisfied and so he complained to this service with the assistance of a representative. He said NatWest did provide a warning when he made the payment of £20,000, but he was entirely under the spell of the scammer, so the warning was ineffective. He said it had multiple opportunities to stop the payments going through and should therefore refund the money he lost.

Mr R's representative said NatWest should have intervened on 6 July 2022 when he made the first payment of £10,000, or on 1 August 2022 when he paid £20,000. They said there were obvious signs the payments were fraudulent including the fact they were large payments to a new payee made in quick succession. And Mr R normally made low payments from the account, so the behaviour was unusual.

They said NatWest should have asked Mr R what the payments were for and whether he'd been approached or offered an investment, which would have led to more questions such as how he found out about P, how P found his contact details, whether he'd researched P, whether he'd checked the Financial Conduct Authority ("FCA") website, whether he'd obtained independent financial advice, whether he'd been asked to download AnyDesk and whether he'd been promised unrealistic returns.

The representative said Mr R wasn't prompted to give false answers, so NatWest would have discovered P had the hallmarks of a scam and properly cautioned him about the prevalence of investment and recovery scams and the risks inherent in making payments to online recovery companies, which would have caused him to reconsider making the payments.

Our investigator didn't think the complaint should be upheld. She noted Mr R was given a new payee warning when he made the first payment of £2,000 on 6 June 2022, which she didn't think was sufficiently tailored. But she didn't think NatWest needed to intervene at that point because the account had history of transactions of similar value, so she was satisfied it had done enough.

The second payment was blocked. Our investigator accepted the payment was unusual and she didn't think the warning NatWest gave during the call was effective as it didn't relate to impersonation scams. But she didn't think it had missed an opportunity to uncover the scam because Mr R didn't disclose the involvement of the third party. And based on what took place during the later calls, she didn't think a better intervention would have made a difference to the outcome.

During the call that took place when Mr R made the third payment, he confirmed he'd received the first two payments into the beneficiary account and denied he'd been put under pressure to make the payment or that he was told to lie. Our investigator didn't think NatWest provided an effective scam warning during the call as it related to a Police/HMRC impersonation scam but based on what took place during the later calls, she didn't think a more effective warning would have made a difference.

In support of these findings, our investigator explained there was a further call on 7 June 2022 when Mr R tried to pay £20,000 to W. During the call he was asked about the loans he'd received and why he was sending funds to W. He said he was transferring money to a friend in Portugal because he was helping him to pay his mortgage. NatWest refused to authorise the payment and asked Mr R to provide details about the reason for the payment. In a further call on 9 June 2022 Mr R said he was helping his cousin to pay for medical expenses. NatWest refused to process the payment and asked him to provide evidence of the hospital bills.

Our investigator explained NatWest should have intervened again on 29 July 2022 when Mr R paid £18,900 as it was a high value payment to a beneficiary it already had concerns with, but she didn't think this would have made a difference as Mr R had gone ahead with the previous payments despite warnings from NatWest and had made payments from his W account totalling £119,000 on 13 June 2022 and 14 June 2022. And once his NatWest account was unblocked, he used that account to make further payments towards the scam.

Mr R has asked for the complaint to be reviewed by an Ombudsman. He has argued that Banking Protocol should have been enacted and NatWest should have called him into the branch to ensure he was fully aware of the decisions he was making, which would have prevented him from making further payments.

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 he's fallen victim to, in all but a limited number of circumstances. NatWest had said the CRM code didn't apply in this case because the payments were to an account in Mr R's own name, and I'm satisfied that's fair.

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 exchanges 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 either of the cryptocurrency exchange companies was fair.

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 this was 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 did enough 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.

Mr R was given a pop-up warning on 6 June 2022 when he set up the new payee and made the first payment of £2,000. I've considered the nature of the payment in the context of whether it was unusual for the spending on the account, and I don't think it was. Mr R paid £14,350 on 15 September 2021, £1,218.30 on 27 September 2021, £1,309.62 on 5 January 2022, £3,800 on 25 February 2022 and £1,099 on 17 May 2022, so £2,000 wasn't unusual and Halifax didn't need to intervene.

Later the same day, Mr R made a further payment of £10,000 and NatWest intervened and asked a series of questions before releasing the payment. I agree with our investigator that the warning wasn't relevant but, considering he wasn't open with the call handler about the purpose of the payment, I don't think it was unreasonable that NatWest failed to provide a more tailored warning.

The second call took place on 6 June 2022 when Mr R made a payment of £8,000. During the call Mr R said he wasn't under pressure from a third party and that he hadn't been told to lie. I've considered the nature of the questions he was asked, and I don't think they were sufficiently robust or probing because he wasn't asked why he was making the payment. However, based on the responses Mr R gave to questions he was asked during the later calls, I don't think he'd have answered truthfully if the call handler had properly questioned him during this call.

When Mr R tried to transfer £20,000 on 7 June 202, the payment was blocked, and he was questioned about the purpose of the payment. Mr R said he was lending money to a friend/cousin in Portugal who needed it for various reasons including paying his mortgage

and the call handler refused to approve the payment. In a further call on 9 June 2022, he said the money was to pay for medical bills for his friend/cousin in Portugal, but he was unable to produce evidence of the medical bills and so the call handler refused to release the payment.

Based on the conversations that took place during the calls Mr R had with NatWest on 7 June 2022, 8 June 2022, and 9 June 2022, I don't think more probing questions on 6 June 2022 would have made a difference to the outcome. This is because when he was asked about the purpose of the payment, he didn't tell the truth and he maintained the explanation in the fact of further questions, meaning it was impossible for NatWest to identify the nature of the scam. For the same reason, while I agree NatWest ought to have intervened on 29 July 2022, I don't think this would have made any difference to the outcome.

Mr R has NatWest should have called him into the branch to discuss the payments, but I don't think this would have made any difference to his decision to go ahead with the payments because he continued to make payments from his NatWest after his account was blocked. He has explained he believed what he was told by the scammers as he had previously invested in cryptocurrency, he was impressed by P's website and had received documentation confirming the agreement. And the scammers called him every day with updates on the progress of his investments which made him feel they a solid working relationship. And because he wasn't honest about the purpose of the payments, I don't think there was anything it could reasonably have done to change his mind.

So, while I think NatWest could have done more when it intervened on 6 June 2022 and that it should have intervened again on 29 July 2022, I don't think this represented a missed opportunity to prevent his loss and so I can't fairly ask it to do anything to resolve this complaint.

Recovery

NatWest didn't attempt to recover the funds because they were sent into an account in Mr R's name and control, and I'm satisfied that was fair because he moved the funds on from his W almost immediately.

Compensation

I'm not asking NatWest to pay Mr R any compensation or legal fees.

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 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 6 December 2023.

Carolyn Bonnell
Ombudsman