DRN-4086155

The complaint

Mr P 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 P saw on social media that a friend had made a few thousand pounds from investing in cryptocurrency. He'd known the person for three years and trusted them implicitly, so he messaged the friend and asked him about the investment. The friend assured him the investment was genuine, claiming he was surprised at the money he was making.

The friend referred Mr P to a broker who seemed professional and had a social media account, which featured photos of her socialising with friends and family. She also detailed her work and what she does to help clients achieve great profits. The page featured positive reviews and several videos of her discussing the logistics of trading.

The broker told Mr P she was happy to coach him on how to invest in cryptocurrency and that he would earn a huge daily profit, explaining she took 15% commission from the total profit. Mr P felt reassured by the fact his friend had recommended the broker and the fact she seemed professional and articulate. He wasn't put under pressure and there was no sense of urgency.

The broker provided a link to 'FinTech' via WhatsApp and instructed Mr P to open an account, stressing the importance of not sharing his log in details with anyone else. He had to go through a security process and was told he could use the account to monitor his trades and make withdrawals and he could see his initial deposit in the account, as well as all open trades the scammer had processed on his behalf.

The broker instructed Mr P to first purchase cryptocurrency through a cryptocurrency exchange company and then load the cryptocurrency onto her online wallet. Between 24 January 2022 and 26 January 2022, he made five payments to two cryptocurrency exchange companies totalling £3,700.

He could see his profits increasing rapidly and submitted a withdrawal request via the trading account. He was asked for an authorisation pin to process the withdrawal and was told to pay a £500 fee to verify the account and withdraw his profits. He then transferred the funds from the cryptocurrency exchange into his trading account, then on to a second digital wallet, as instructed by the scammer. The broker confirmed the funds had been received and that she would action withdrawal.

On 25 January 2022, the broker contacted Mr P claiming the withdrawal had been delayed due to unpaid fees. She said the funds had been successfully withdrawn from the trading

account into Ms P's bank account and suggested they had been held by the 'Internal Revenue Code', as they were asking investors to pay a transaction fee and 15% tax.

Mr P contacted his friend via social media to question the process and was reassured that it was normal. The broker told Mr P he'd need to pay £2,000 in fees, but he said he didn't have the money. He eventually agreed to pay the fees and split the payment into two payments of £1,548 and £451 due to limitations on how much he could transfer. The broker then told him to pay her commission fee of £1,000 and that there was no option for this to be taken out of his profits. He agreed this after more reassurance from his friend.

When he didn't receive any money, he received a message from the broker claiming his account had been frozen and that he must pay £250. At this point he realised he'd been the victim of a scam and his friend told him he hadn't been sending the messages.

Mr P complained to NatWest, but it said it couldn't refund any money because the transfers were to an account in Mr P's name. It explained it places warning messages across its online banking facility to warn customers about scams and, before payments are processed, a message is displayed warning customers about scams. It explained its fraud system monitors activity for the latest fraud trends and if a transaction matches a known trend, a security check will be generated. The payments didn't match any fraud trends and were not deemed as suspicious, so a security check wasn't generated.

It accepted the customer service Mr P received when he reported the scam fell below a reasonable standard and apologised for that. And it maintained there were no blocks or restrictions as the payments weren't suspicious.

Mr P wasn't satisfied and so he complained to this service. He said he didn't question what he saw on his friend's social media account because he trusted him and assumed it was genuine. The tone of the subsequent conversations was exactly the same as previous interactions and he was persuaded by the professional-looking social media page and the fact the broker was transparent about her fees He explained he didn't have any investment experience so he didn't understand the sort of due diligence he should have done, and he said that apart from biometric checks, the payments went through without any intervention from NatWest.

Mr P's representative argued that even though the transfers were 'me to me', they were unusual, and NatWest should have intervened. They said that if it had asked Mr P about the payments, it would have been apparent he was falling victim to a scam and, but for its failure to make further enquiries, it would have been on the actual notice that he was going to suffer financial harm.

They argued NatWest should have asked Mr P what the payments were for and the basic surrounding context and it's likely he'd have explained what he was doing and that everything had originated from a "broker". And whilst the money was being sent to legitimate cryptocurrency exchanges, NatWest should have still provided a scam warning in light of all the information known to banks about the increasing number of scams associated with cryptocurrency. They further argued that on the one occasion Mr P spoke to NatWest, it failed to detect the scam and that the activity was unusual for the account, so it ought to have questioned what was happening.

Our investigator didn't think the complaint should be upheld. He noted all the payments were to legitimate cryptocurrency exchange companies and there was nothing which should have caused NatWest to intervene and provide a scam warning.

Mr P has asked for the complaint to be reviewed by an Ombudsman. His representative has argued it's well known that scammers groom consumers into setting up accounts with genuine cryptocurrency companies and then have move the cryptocurrency to a wallet under the guise of a trading platform. They have said Mr P didn't have a history of investing and the value of the payments is significant in comparison to his usual spending.

Specifically, they have said NatWest should have intervened when Mr P tried to make the third payment of £1,549 because it was a sudden unusual change in Mr P's regular expenditure and it was well known that the two cryptocurrency exchanges are used by scammers.

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 P 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.

I'm satisfied Mr P '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 P 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 P 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 genuine cryptocurrency exchange companies. 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 P 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 P from financial harm due to fraud.

I've considered the nature of the payments in the context of whether they were unusual or uncharacteristic of how Mr P normally ran his account and I don't think they were. All the payments were to legitimate cryptocurrency exchange companies and none of them were for

particularly large amounts, nor were they out of character for the usual spending on the account. Mr P had made a payment of £2,149 on 25 November 2021 and the largest of the disputed payments was £1,549 on 25 January 2022, so it wasn't not unusual. And even though the payments were linked to cryptocurrency investing, this doesn't mean they were suspicious. So, I don't think NatWest missed an opportunity to intervene.

Chargeback

I've thought about whether NatWest could have done more to recover Mr P'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 P).

Mr P'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 P'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 Mr P 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 P to accept or reject my decision before 6 October 2023.

Carolyn Bonnell
Ombudsman