DRN-4440948

The complaint

Ms F 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 October 2021, Ms F was looking to invest in cryptocurrency as she had some friends who had made some profit from it. Her friends were actioning their own trades and investments but as she had no prior knowledge of cryptocurrency, she wanted to find an agent or broker to help her.

She read an article online which included a link to a platform that she understood would put her in touch with a broker. She registered her interest and was subsequently contacted by an agent who did a full security check and asked for photo ID to verify her identity. During the call Ms F was given a code and told that if she ever received a call about the investment, she should ask the caller for the code. She was then told she would be contacted by an appropriate investment company.

Two days later, Ms F was called by someone claiming to be a broker who worked for a company I'll refer to as "M". He quoted the security code and sounded friendly, professional, and extremely knowledgeable about investing. The broker told Ms F she'd need to make an initial deposit of £200 to open an account. He explained the process and said he'd place trades on her behalf, taking a commission cut of 2.5% of her profits.

Before going ahead with the investment, Ms F carried out some due diligence and found some reviews online which were mostly positive. There were some negative reviews, but she felt this was believable. She also checked M's website, which was slick and professional, and featured profit and loss charts and graphs showing the fluctuating market performance of different currencies.

On 11 October 2021, Ms F used her debit card to pay £189.13 to open an account. The broker told her to download Anydesk so he could take control of her trades and that she should purchase cryptocurrency through a cryptocurrency exchange company and then load the cryptocurrency onto her online wallet.

Following the initial payment, Ms F spoke to the broker regularly. Around the beginning of November 2021, he told her there would soon be major movement in the market and he'd get a loan of £20,000 from M, which he could use to demonstrate how he could generate profit. Ms F could see the loan generated around £60,000 profit within a week, which she didn't think was unreasonable or unrealistic based on stories she'd heard of people making life-changing sums of money from investing in cryptocurrency.

The broker told Ms F she could make a withdrawal, but she'd have to pay the loan back. He

advised her to invest £20,000 to pay back the loan, and a further £4,000, which would gain her an additional "bonus" and elevate her account to "gold" status. He assured her that if something went wrong, he'd send the money from his own bonus account.

Ms F tried to transfer £17,000, but the payment didn't reach the broker's account and when she discussed this with broker, he said NatWest didn't like people sending money to investment companies and told her to send money from the account she held with "W". On 25 November 2021, she sent £20,000 to W, followed by £4,000 on 26 November 2021.

Neither payment was flagged for security checks and Ms F immediately saw a £4,000 bonus payment on her trading account. But shortly afterwards she lost contact with the broker, and she eventually realised she'd been scammed.

Ms F complained to NatWest, but it said the payments were to an account in her own name, so it wasn't the point of the loss. It said it places appropriate and relevant warning messages across its online banking facility to warn customers about scams and that the information is available on its websites and in its branches. And that before making a payment, a scam warning is displayed on its online banking facility and these messages are displayed before making a transfer or adding a new payee.

It said the disputed payments didn't match any fraud trends and weren't deemed suspicious, so there were no blocks or restrictions applied. And there was no evidence that the card payment was brought to its attention at the same time as the bank transfers, so a chargeback request would be out of time.

Ms F wasn't satisfied and so she complained to this service. She argued that if NatWest had identified the payments as unusual and suspicious and asked relevant probing questions, it would have become apparent she was falling victim to a scam. Her representative said NatWest should have identified the payments as unusual and suspicious given the amounts and the fact the payees were linked to cryptocurrency, and but for its failure to make further enquiries, it would have been on notice that Ms F was going to suffer financial harm.

The representative said that if NatWest has asked Ms F what the payments were for and the basic surrounding context, it's likely she'd have fully explained what she was doing and that everything had originated from the "broker". So, even though she was sending money to a legitimate cryptocurrency exchange company, it should have still provided a scam warning.

NatWest maintained it wasn't the point of loss. It said Ms F had made large payments, some of which related to cryptocurrency, and she didn't heed any of the online warning messages displayed prior to making the payments via her online banking platform.

My provisional findings

I thought about whether NatWest could have done more to recover the debit card payment. 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 (Ms F).

Ms F's own testimony support that she 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 Ms F's payments, they converted and sent an amount of cryptocurrency to the wallet address provided. So, any chargeback was destined fail, therefore I was satisfied that NatWest's decision not to raise a chargeback request was fair.

I was satisfied Ms F '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 F 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 carefully considered the circumstances, and I was persuaded the broker was operating as part of a scam. But, although Ms F didn't intend her money to go to scammers, she did authorise the disputed payments. NatWest is expected to process payments any 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 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'd 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 needed to consider whether it ought to have intervened to warn Ms F when she tried to make the payments. If there are unusual or suspicious payments on an account, I would expect NatWest to intervene with a view to protecting Ms F from financial harm due to fraud.

The payments didn't flag as suspicious on NatWest's systems. I considered the nature of the payments in the context of whether they were unusual or uncharacteristic of how Ms F normally ran her account and I thought they were. Both payments were to a legitimate cryptocurrency exchange company, but they were for large amounts, which was out of character when compared to the usual spending on the account. So, I thought NatWest missed an opportunity to intervene and that it should have blocked the payment and contacted Ms F on 25 November 2021.

I explained that during the call, I would expect NatWest to have asked Ms F some probing questions around whether there was a third party involved, how she met the third party, whether she'd been promised an unrealistic rate of return and whether she'd given anyone else control of her trading account. I would also expect it to have discussed the checks she'd done and provided a full scam warning.

Our investigator didn't think Ms F would have been open in her response to questioning, citing evidence that the broker told her that banks don't like customer's sending money to cryptocurrency exchange companies, which is why she then transferred the money via the account she held with W. But I had listened to a call dated 27 October 2021 when Ms F

discussed with NatWest the fact it didn't authorise payments to cryptocurrency exchange companies and that she'd tried to get around that by reducing the amount and paying by card. This made me think she would have been honest with NatWest had it contacted her on 25 November 2021.

Because of this, if NatWest had intervened and asked robust questions, I thought it would probably have gathered enough information to suggest this might be a scam, including the fact Ms F was being advised by a broker she'd found online who'd advised her to download remote access software and the fact she'd been told to transfer money via the account she held with W. And I would expect NatWest to have warned Ms F that the investment had the hallmarks of a scam.

Ms F had said she trusted the broker because he seemed genuine, and she was encouraged by the fact her initial investment produced a profit. But if NatWest had warned her that the investment had the hallmarks of a common cryptocurrency scam and that £60,000 profit within a week was implausible, I thought she'd have thought twice about what the broker had told her. And I was satisfied that, while there were no warnings about M on the FCA or IOSCO websites, if Ms F had known she could be the victim of a scam, she would have thought twice about going ahead with the payments as there's no evidence that she was keen to take risks with her money. So, I was minded to direct NatWest to refund the money Ms F lost from the second payment onwards.

Contributory negligence

I accepted there's a general principle that consumers must take responsibility for their decisions and conduct suitable due diligence but, in the circumstances, I didn't think Ms F was to blame for the fact she didn't foresee the risk.

In recent years instances of individuals making large amounts of money by trading in cryptocurrency have been highly publicised to the extent that I didn't think it was unreasonable for Ms F to have believed what she was told by the broker in terms of the returns she was told were possible, notwithstanding the fact it was highly implausible.

Ms F hadn't invested in cryptocurrency before and so this was an area with which she was unfamiliar. She wouldn't have known the returns were unrealistic or how to check the information she'd been given. This unfamiliarity was compounded by the sophisticated nature of the scam, the fact she trusted the broker and the fact she believed the trading platform was genuine and was reflecting the fact her investments were doing well. So, I didn't think she could fairly be held responsible for her own loss.

Developments

Ms F has said she accepts the findings in my provisional decision.

NatWest suggested the online banking audit should be reviewed to ascertain in which order the payments were made, but it hasn't produced this evidence.

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.

Ms F's statement shows the payments were made on three different dates and as NatWest hasn't provided any evidence to the contrary, I'm satisfied that is what happened.

Because NatWest hasn't made any further comments or added anything which might alter my view, the findings in my final decision will be the same as the findings in my provisional decision.

My final decision

My final decision is that National Westminster Bank Plc should:

- refund £24,000.

- pay 8% simple interest*, per year, from the respective dates of loss to the date of settlement.

*If National Westminster Bank Plc deducts tax in relation to the interest element of this award it should provide Ms F with the appropriate tax deduction certificate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms F to accept or reject my decision before 4 December 2023.

Carolyn Bonnell
Ombudsman