DRN-3997633

The complaint

Miss F complains that Barclays Bank UK 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.

Miss F complains that Barclays won't refund the money she lost to an investment scam. In October 2020, Miss F was approached by a close family friend who she'd known for over 15 years. The friend told her he'd made good profits from investing in cryptocurrency and explained there was an upcoming zoom presentation for prospective investors which she should attend.

The presentation hosted by a company I'll refer to as "B". There were 10 attendees and the presenter appeared very professional. The presenter explained B offered investments in up to 24 different currency pairs, 9 stocks including Google and Tesla, and 9 cryptocurrencies and was registered under the Australian Investment and Security Commission (ASIC). The presenter showed testimonials of previous success stories and explained it was possible to earn a commission from making successful referrals to new investors.

After the presentation, Miss F checked B was registered on the ASIC. She also found B's social media channel, which featured a video from the Chief Operating Officer, and she accessed the website which included a live trading room, an online chat facility, and sections on 'Know Your Customer' and Anti Money Laundering policies. There were no negative reviews online.

Before going ahead, Miss F contacted her friend to ask further questions including how long he'd been investing with B, whether he'd been able to withdraw any money and whether he would recommend the company. Miss F then used the referral link to access the trading site and register an account, a process which required her to submit her personal details and submit photo ID and proof of address. Within 24 hours, the identification checks were complete, and Miss F received log-in details to her trading account.

Miss F was told to first purchase cryptocurrency through a cryptocurrency exchange company and then load the cryptocurrency onto her online wallet. She was added into a WhatsApp group by her friend with the people who'd attended the presentation. She made a small initial payment in October 2020 and could immediately see profits on her trading account. She felt the rate of return was plausible and the broker was responsive and knowledgeable, dealing with queries in a timely manner. Between 2 November 2020 and 8 December 2020, she made seven further payments of £2, £250, £300, £300, £300, £200, and £200 from an account she held with another bank.

On 29 December 2020, Miss F was given the option to cash her investments in or re-invest the money, so she issued a withdrawal request for £2,263.27. Within an hour, the money

was available, and she transferred it to her current account. On 5 January 2021 Miss F submitted another withdrawal request and received £1,193.21. On 6 January 2021, she invested £300 and on 13 January 2021, she withdrew a further £1,806.46.

On 25 January 2021 and 4 February 2021, Miss F made payments of £2 and £7,000 from her Barclays account. These were the only payments from her Barclays account. The payment was initially blocked by Barclays and in the subsequent phone call, Miss F was asked where the money was being sent to and if she felt she had been coerced into making the payment. She confirmed the funds were being sent to a cryptocurrency exchange company and she was acting independently.

Over the next few weeks Miss F made two more payments and received several withdrawals. But in March 2021, she noticed she was unable to access her trading account and was told this was due to maintenance on the website. She was then given a variety of reasons as to why investors could not access their accounts and eventually lost access to her trading account. She then discovered publications stating that B was fraudulent, and she realised she'd been scammed.

Miss F complained to Barclays, but it said it was unable to review the claim because she'd failed to report it to the fraud team. She wasn't satisfied and so she complained to this service with the assistance of a representative. The representative explained that even though there was a call after the £7,000 payment was blocked, Barclays didn't ask probing questions around the purpose and intended destination of the payment and she wasn't given an effective warning.

They said Barclays failure to make further enquiries meant it wasn't on notice of the purpose of the payments and that it failed to intervene in circumstances which might have prevented the scam. They said that Miss F would have fully explained what she was doing and that everything had originated from a broker and that even though she was paying a legitimate cryptocurrency exchange company it should have still provided a scam warning.

The representative argued the payments were extremely unusual for Miss F as she barely uses the account and that if Barclays had identified the payment as unusual and suspicious and asked relevant questions, it would have been apparent that she was failing victim to a scam.

Barclays commented that the payments were sent to a wallet held by Miss F in her name which she had control of and that the Contingent Reimbursement Model ("CRM") code didn't apply because it was to an account in her own name. It also said that when she made the first payment, she selected 'something else' rather than 'Investment of crypto-currency'. It said it blocked the payment because it was out of character and that if she'd selected the correct purpose, it could have provided her with the correct warning, which may have prompted her to make additional checks as well as the ones she already had conducted.

Our investigator didn't think the complaint should be upheld. He said B was likely a pyramid scheme where investors can earn money via introducing others to the scheme, or by their own investments and he was unable to satisfactorily that the evidence payments were paid to B from cryptocurrency exchange company, so he couldn't conclude it was a scam. He was also satisfied Barclays had given Miss F a warning, after which she chose to go ahead with the payment.

Miss F has asked for the complaint to be reviewed by an ombudsman arguing that they have done all they can to show the cryptocurrency was transferred to the scammer's wallet given the circumstances and in other cases, showing statements for the cryptocurrency exchange platform has been enough.

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 know 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 Miss F says she's fallen victim to, in all but a limited number of circumstances. Barclays had said the CRM code didn't apply in this case because the disputed payments took place before the code came into force, and I'm satisfied that's fair and applies to all of the four bank transfer payments.

I'm satisfied Miss 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, she 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).

Our investigator wasn't satisfied that Miss F has shown funds were transferred from the account she held with the cryptocurrency exchange company to an account controlled by scammers. She has given a detailed account of the circumstances around her loss and she had submitted some material about B. But our investigator was able to find this material online and I agree with him it doesn't constitute evidence that Miss F lost money to B.

Such evidence might include emails or whatsapp/text messages between Miss F and the scammers, which she hasn't produced. She also hasn't been able to provide any evidence of chats with the friend who introduced her and, given she paid a cryptocurrency provider in her own name, it seems very odd that she's unable to provide any form of statement of account, or evidence to show she paid away the cryptocurrency she purchased.

Further, she didn't tell Barclays this was anything other than a personal investment when it blocked the payment and it's reasonable to expect she would have done were it her intention to pass it to B.

In light of all of that, I'm not persuaded Miss F has suffered a loss and so I can't direct Barclays to do more.

My final decision

My final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss F to accept or reject my decision before 10 October 2023.

Carolyn Bonnell
Ombudsman