DRN-4193092

The complaint

Mr H complains that Barclays Bank UK 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.

In January 2021, Mr H received a marketing email from a company I'll refer to as "T", introducing themselves as brokers who specialised in cryptocurrency investments. Mr H was sent a link to T's website which featured its T&Cs, and a certificate of its registration with the Global Financial Authority ("GFA").

Mr H looked T up on Trustpilot and saw it had a three-star rating. There were some negative reviews, but after speaking to one of T's brokers, he was satisfied they'd been posted by people who had deposited small amounts and were unhappy with the returns. The broker explained T was based in Switzerland and didn't need to be regulated by the FCA. He said fees and taxes would need to be paid before Mr H could make withdrawals, and that he'd be able to withdraw a monthly dividend when the account balance reached £30,000.

The broker advised Mr H to download Anydesk and then purchase cryptocurrency through a cryptocurrency exchange company before loading it onto an online wallet. Between 26 May 2021 and 16 August 2021, he made 21 payments to three cryptocurrency exchange companies totalling £561,750 using a visa debit card and online transfers from his Barclays account. Our investigator subsequently found there were more payments, but Mr H doesn't want those payments included in this complaint.

When the balance on the trading account reached £16,000,000, Mr H decided to make a withdrawal, but the request was rejected. The broker told him he'd have to pay withdrawal fees, which he paid with a director's loan from his company. But once he'd paid the fee, Mr H was told it had been paid to the wrong person and, when he refused to pay more, he lost contact with the broker, at which point he realised he'd been the victim of a scam.

Mr H complained to Barclays, but it said it was unable to refund any of the money he'd lost. It accepted there were issues with the service he'd received, offering an apology and £300 compensation. But it said that as the money was lost from a cryptocurrency wallet in his name, the claim fell outside of current Contingent Reimbursement Model (CRM) guidance.

It said that, given the large amounts of money sent during the scam period, Mr H hadn't done sufficient due diligence. and he should have taken independent advice from a qualified or registered financial expert, having instead put most of his faith in information provided to him by the scammers. It also said he'd knowingly allowed remote access software to be installed and had followed the guidance of the scammers when setting up various cryptocurrency wallets. He'd gone ahead in the face of negative reviews, the apparent returns on the investment were far too good to be true, and during calls with its fraud team,

Mr H had spoken openly and with confidence and authority about the investment and the various processes involved.

Mr H wasn't satisfied so he complained to this service. He said the payments were much larger than his normal account activity and he had researched T, but didn't find any adverse information until after he realised he'd been scammed. And he didn't check the FCA register as he's not an experienced investor.

Our investigator didn't think the complaint should be upheld. She explained the Contingent Reimbursement Model Code ("CRM") didn't apply to card payments or international payments, and all the disputed payments were to accounts in Mr H's name, so the code wouldn't apply. She said chargeback was relevant as one of the payments was made using a Visa debit card, but Mr H couldn't have a valid claim against the legitimate company he paid because it had provided the services as intended, which was to purchase the cryptocurrency and transfer to a wallet.

Our investigator said there were reasonable grounds for Barclays to have intervened, explaining the frequency of the payments and sums involved in relation to how much Mr H normally spent meant it ought to have identified this was a highly unusual and uncharacteristic pattern of spending. She didn't think the first two payments on 26 May 2021 were unusual because Mr H had opened the account on 21 May 2021 for the purpose of investing, so there was no spending history to compare with, and there were sufficient funds to facilitate the payments. But she thought the third payment of £9,500 was unusual because it was the third consecutive payment of high value that he'd made in under three minutes, and it was to a high-risk merchant.

She noted Barclays had called Mr H on 26 May, 22 June 2021, and 28 July 2021, but there was no evidence he'd been given a full scam warning on any of those occasions. However, she didn't think it would have made a difference to Mr H's decision to go ahead with the payments if Barclays had given a scam warning during any of those calls, because she didn't think it could have said anything which would have dissuaded him from going ahead with the investment.

This is because, during the interactions Mr H had with Barclays on and after 14 August 2021, while he did say he was buying cryptocurrency, he didn't mention T. And when asked if he'd checked the FCA website, he said he was confident the business he was paying didn't need to be authorised and that he was simply transferring cryptocurrency into a wallet.

Further, our investigator didn't think a full scam warning during that or any of the earlier calls would have prevented Mr H from going ahead with the payments because in a call with a different bank on 27 April 2021 where he did disclose T's involvement, he was told about an FCA warning dated 12 February 2021, and continued to make further payments both from that account and his Barclays account. Our investigator also referred to messages Mr H had with the scammers which suggested people around him had concerns T was operating a scam, and he still went ahead.

So overall, our investigator didn't think an earlier or better intervention would have made a difference to Mr H's decision to go ahead with the investment and so it wouldn't be fair to hold Barclays liable for his loss.

Finally, our investigator said there was no evidence Barclays had contacted the beneficiary banks to attempt to recall any funds, but as they were paid into accounts in Mr H's own name before being moved on to the scammers trading platform, it's unlikely it would have been able to recover any of the funds. She explained Barclays had acknowledged there were customer service issues and had paid £300 compensation and she was satisfied that

was fair because when he reported the scam, there was nothing it could do to recover his money.

Mr H wasn't satisfied and has asked for his complaint to be reviewed by an Ombudsman, questioning how our investigator could conclude Barclays should have intervened sooner, but that it wouldn't have made any difference.

He's argued he was groomed by a sophisticated scam, and yet Barclays did nothing to protect him. He's said what he said during the calls with Barclays was misplaced confidence and that before his contact with T, he had no knowledge of trading, meaning he was vulnerable and at risk.

He's said he trusted Barclays to exercise due diligence and take proactive measures to protect his interests and financial well-being. And that the presence of unusual activity should have prompted it to initiate a comprehensive review, including gathering additional information from him and conducting necessary investigations to confirm the legitimacy of the transactions. He's argued that by neglecting to take appropriate action, Barclays allowed the fraudulent activity to persist and by neglecting to intervene and investigate the unusual activity on his account, it contributed to the financial loss and distress he's experienced.

He's said there were numerous irregular and unusual payments from his account, which were clearly outside the scope of his normal financial behaviour, and which should have raised immediate concerns. He maintains he had had no prior experience with cryptocurrency exchanges before encountering the scammers and, as an inexperienced investor, he relied on the assurances and recommendations provided by Barclays, entrusting it to guide him safely and responsibly through the process. He's said he fell victim to an intricately engineered scam that capitalized on his lack of knowledge and experience and the scammers employed sophisticated tactics to deceive him and manipulate his actions.

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

I'm satisfied Mr H '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, he 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 H didn't intend his money to go to scammers, he did authorise the disputed payments. Barclays 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 Barclays 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, Barclays 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 H when he tried to make the payments. If there are unusual or suspicious payments on an account, I'd expect it to intervene with a view to protecting Mr H from financial harm due to fraud.

Barclays blocked payments on 26 May 2021, 22 June 2021, and 28 July 2021, but we only have a call recording for the intervention that took place on 28 July, during which Mr H was asked to confirm the payment was genuine. And, in the absence of evidence of what took place during the other two calls, I'm satisfied those payments were probably also released without adequate questioning or a scam warning.

The next intervention took place on 14 August 2021, when there were three separate calls. During these calls, Mr H engaged in detailed conversations about the fact he was simply buying cryptocurrency to keep in his wallet. He explained he'd moved cryptocurrency he already held and was buying more from other sellers. He said that even if the price of cryptocurrency fell, he wouldn't lose money unless he sold it. Critically, he told Barclays there was no third-party involved, that he hadn't been promised a guaranteed return and that he knew he could lose money. During the calls, he was told to check the FCA register and was warned about the risk of scams.

I've thought about whether Barclays ought to have given Mr H a fraud warning earlier than 14 August 2021 and in doing this I've considered the nature of the payments in the context of whether they were unusual or uncharacteristic of how Mr H normally ran his account. All the payments were to legitimate cryptocurrency exchange companies, but they were for very large amounts, and I agree with our investigator that he should have been given a full scam warning during the call that took place on 26 May 2021.

I also think Barclays should have intervened again when Mr H paid £42,500 on 27 May 2021. I accept that by this time Mr H had paid the payee on four previous occasions, but there's no evidence he'd been given a full scam warning at this point and as the payment was high-value, Barclays should have stepped in and questioned him around the purpose of the payments and the nature of the checks he'd made. It should also have warned him about the risks associated with the investment and given examples of the types of scams to look out for.

I've also considered the nature of the warnings Mr H was given during the calls that took place on 14 August 2021, and I don't think Barclays did enough. During the calls, Mr H sounds as though he knows exactly what he is doing but I think the call handlers should have taken control of the calls and given more information about red flags he should be looking out for. Mr H repeatedly said there was no third-party involved, but considering the

size of the payments, I think he should have been pushed on the point and warned that it would be a red flag if he'd been approached by a third-party or advised to use remote access software.

However, I'm satisfied that, even if Barclays had been more robust in its questioning, it's unlikely Mr H would have disclosed T's involvement, so there's no way it could reasonably have uncovered the fact he was being scammed based on the information it had. Further, even Mr H had been open about T's involvement, I don't think it would have made any difference to the outcome. This is because I've listened to the call that took place between Mr H and his other bank on 27 April 2021. In that call, there was a discussion about T during which Mr H was told about the FCA warning dated 12 February 2021, and he still went ahead with the investment. And the fact he went ahead having been told about the warning means it's more likely than not that any warning Barclays might have given would have been met with the same response.

Mr H was very confident the investment was genuine and decided to go ahead, notwithstanding a warning from the FCA that pre-dated the payments, and multiple scam warnings from both banks. It's also worth noting that he opened the Barclays account for the purpose of continuing the investment after he had the scam conversation with the other bank. In these circumstances, even though I agree with our investigator that Barclays could have done more to warn Mr H, and that it should have been done sooner, I don't think it would have made a difference.

Chargeback

I've thought about whether Barclays could have done more to recover Mr H'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. Barclays) acted fairly and reasonably when presenting (or choosing not to present) a chargeback on behalf of its cardholder (Mr H).

Mr H'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 H'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 Barclay's decision not to raise a chargeback request against any the cryptocurrency exchange companies was fair.

Overall, I'm sorry to hear Mr H has lost money and the effect this has had on him. I do think Barclays could have done more sooner, but for the reasons I've explained, I don't think it could have prevented Mr H's loss 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 H to accept or reject my decision before 17 October 2023.

Carolyn Bonnell
Ombudsman