DRN-4331433

The complaint

Mr P complains that Barclays Bank UK PLC didn't do enough to protect him from the financial harm caused by two investment scams, 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.

Mr P was researching investment opportunities and came across an advert on social media regarding an opportunity to invest in cryptocurrency which was endorsed by a well-known celebrity and involved two companies which I'll refer to as "G" and "C".

Scam 1

Mr P was contacted by someone I'll refer to as "the scammer" who explained how to set up a trading account with C. The scammer said he would have to pay £250 and asked him to provide photo ID. He said he would be provided with log in details and asked him to download AnyDesk remote access software. The scammer seemed professional and knowledgeable and showed Mr P how to navigate the website so he could keep track of his investments and make withdrawals.

The scammer asked him to first purchase cryptocurrency through a cryptocurrency exchange company and then load it to an online wallet. Mr P transferred £250 from his Barclays account on 29 July 2022, but on 12 August 2022 he saw that this account was frozen. The scammer told him to make a small investment to ensure the account was running correctly, so he made a further payment of £10.

On 31 August 2022, Mr P noticed the trading account wasn't working again and so he contacted the scammer who told him there was a technical issue. When he still couldn't access the account, he was told the account was in deficit and that he'd need to invest £6,000 to re-balance the account.

Mr P made the payment on 7 September 2022 and the account was re-opened. He noticed the balance was less than he expected but the scammer said he'd made a profit on the initial investment and it was now showing a total sum of £26,000. Mr P then asked to make a withdrawal but the scammer said this wasn't possible because trading levels were down. The following day he realised his account had been closed again and he couldn't get in touch with the scammer, at which point he realised he'd been scammed.

Scam 2

On 29 July 2022, Mr P also invested £250 with G. He then contacted by someone who I'll refer to as "the scammer" who sent him a link to his trading account and a secure code. He

also told him to download AnyDesk and sent him screenshots with regards to the potential profits and an overview on the market progress.

The scammer asked Mr P to first purchase cryptocurrency and then load it onto an online wallet. Before investing further, he researched G, noting the website was professional and that there was nothing of concern.

The scammer told Mr P he'd need to pay a further £2,000 to invest in the Bronze Platform and activate the account and that he could invest up to £10,000 before moving on to the Silver Platform, which he was encouraged to do because it would generate greater profits. But when he came to request a withdrawal he was told he'd have to pay £7,311 in taxes. He realised he'd been scammed when the scammer said that if he invested a further £20,000, he would pay £100,000 into his account.

The complaint

Between 29 July 2022 and 9 September 2022, Mr P made five debit card payments and nine debit card payments to the scams totalling £66,301. He complained to Barclays when he realised he'd been scammed. It apologised for the customer service he'd received and paid him £50 compensation, but it refused to refund any of the money he'd lost.

It accepted it hadn't intervened in any of the payments but it said the payments were in line with the previous spending on the account and the funds were being sent to an account in Mr P's own name, so they weren't flagged by its fraud prevention system.

It also said that a search of C brought up several warnings pre-dating the scam and that Mr P had failed to complete reasonable due diligence because he didn't take independent advice or do any research, instead relying on the word of the scammer.

Mr P wasn't satisfied and so he complained to this service with the assistance of a representative. The representative said Barclays had failed to raise a chargeback request and that it should have intervened as Mr P made fourteen payments to a new payee with links to cryptocurrency within six weeks.

They said Mr P used the account for general spending and the largest payment on the account was £5,000 to his wife on 28 April 2022 and a transfer from one of his other accounts the same day. In May 2022, he paid £5,000 to his wife and the next largest payment was £886.16 on 3 May 2022. In June 2022 the largest payment was £5,000 on 1 June 2022, followed by £2,415.69 on 30 June 2022.

The representative argued that multiple large payments to a new cryptocurrency merchant within a short space of time should have been a red flag. They said it should have contacted Mr P before the first payment to ask him why he was making the payment, how he found out about the company, whether he'd researched the company, whether he'd been promised unrealistic returns, whether he'd made any withdrawals and whether he'd been pressured to make the payment. And had it done so, a properly trained member of staff would have immediately picked up the scam and provided appropriate advice which would have prevented further loss.

Barclays said it was out of time to dispute the transactions using the VISA Chargeback Scheme and there was no reason code which would have led to a refund of the payments to the cryptocurrency exchange as Mr P had received the cryptocurrency he paid for. It said the debit card transactions were out of the scope of the Contingent Reimbursement Model ("CRM") code and as the transfers were all sent to a digital wallet in Mr P's own name, they

were out of the scope of the code. It said it tried to recovered the funds on 2 December 2022 but no funds remained.

It maintained the payments weren't out of character compared to those in the previous six months and Mr P had made multiple payments using Barclays Mobile Banking ("BMB") prior to scam payments. It also said Mr P has given the wrong payment purpose on 15 August 2022 and he had believed the information he'd seen on social media even though the celebrity has publicly stated that any advert he's associated with is a scam.

Our investigator didn't think the complaint should be upheld. He explained that neither the debit card or BMB payments would be covered under the CRM code because the code doesn't apply to debit card payments or payments to accounts in the consumer's own name. He also explained that by the time Mr P referred his complaint this service, he would have been out of time to raise a chargeback request.

He didn't think Barclays had missed an opportunity to intervene because the payments were in line with the normal spending on the account. He explained he'd reviewed Mr P's bank statements for the 12 months prior to the disputed transactions and while some of the disputed transactions were high value, he didn't think Barclays missed an opportunity to intervene because the amounts weren't out of character. Finally, he was satisfied Barclays had tried to recover the funds from the recipient accounts and that no funds remained.

Mr P has asked for his complaint to be reviewed by an Ombudsman. His representative has argued that making multiple payments in one day totalling £18,000 to a relatively new high risk payee with links to cryptocurrency should have triggered an intervention from Barclays. They've argued that the examples of Mr P making multiple payments in one day were to a pre-existing payee and were low value.

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.

The CRM Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Mr P says he's fallen victim to, in all but a limited number of circumstances. Barclays has said the CRM code didn't apply in this case because Mr P was paying an account in his own name, and I'm satisfied that's fair.

I've thought about whether Barclays could have done more to recover the card payments when Mr P 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 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 Barclays decision not to raise a chargeback request against either of the cryptocurrency exchange companies was fair.

Further, the scheme sets the rules and there are specific time limits that must be applied. Those rules state that a claim can be brought no later than 120 days than the date of the transaction. In Mr P's case, the claim was referred to Barclays after this time, so this wasn't an option for Mr P.

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, he is presumed liable for the loss in the first instance.

There's no dispute that this was a scam, but although Mr P 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 a genuine cryptocurrency exchange company. However, Barclays ought to fairly and reasonably be alert to fraud and scams and these payments were part of wider scams, 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 Barclays to intervene with a view to protecting Mr P from financial harm due to fraud.

The payments didn't flag as suspicious on Barclays's systems. 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. The first seven payments were low value and so there would have been no reason for Barclays to intervene. I accept the payments he made to the scam between 29 August 2022 and 9 September 2022 were high value, especially on 29 August 2022 when the cumulative total of two payments was £18,470, but when compared to the previous spending on the account, I don't think the sums were unusual.

On 28 February 2022 Mr P made payments of £3,000 and £5,000, on 1 April 2022 he made payments of £5,000 and £6,000, on 28 April 2022 he made payments of £5,000 and £7,000 and on 7 July 2022 he made a payment of £15,000. So even though the amounts of the scam payments had increased significantly, it wasn't to the extent that the amounts were unusual for the account.

Significantly, the highest single payment to the scam was lower than £15,000 and while I accept the cumulative total of the payments on 29 August 2022 was £18,470, when compared to a single payment of £15,000, I don't think this was concerning, especially as by this time C wasn't a new payee. So, I don't think Barclays missed an opportunity to intervene.

Compensation

Barclays accepts the customer service it provided when delivering the outcome of Mr P's complaint fell short because a detailed explanation as to why the dispute hadn't been upheld should have been given. But it apologised for that and paid him £50 compensation which I'm satisfied is reasonable and addresses the impact its failings had on him.

Recovery

I'm satisfied Barclays tried to recover the funds from the recipient accounts and that no funds remained.

Overall, I'm satisfied Barclays 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 Barclays is to blame for this and so I can't fairly tell it to do anything further to resolve this complaint.

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 X to accept or reject my decision before 8 April 2024.

Carolyn Bonnell
Ombudsman