

The complaint

Ms H complains that Barclays Bank UK Plc ('Barclays') won't refund the money she lost when she fell victim to a scam.

What happened

In April 2024 Ms H was looking online for a part time job to increase her income. She saw an advert on a social media site promoting an opportunity, completed a form and later received a text message with more details.

Ms H was told that she would earn commission by completing tasks such as reviewing items to help increase sales and promoting the products online. The opportunity was presented as being for a well-known retailer and the platform included genuine looking branding. Ms H had to purchase tasks and was told that when she completed sets of tasks she'd receive her money back along with commission earned.

Ms H is disputing 27 payments she made from her Barclays account coming to a total of £28,139. Ms H has said most of the money lost came from her savings, but some came from her family's savings, and she borrowed some money from other family members towards the end.

I haven't listed the payments as they are well known to both parties. In summary, the first 11 payments were card payments to Ms H's own account with an e-money account provider I'll call "R". These payments were made between 13 April 2024 and 16 May 2024 and ranged between £20 and £900. The remaining 16 payments were faster payment transfers from Ms H's Barclays account to an account in the name of a business. These payments were made between 17 May 2024 and 10 June 2024 and ranged between £409 and £2,800.

Ms H says realised she was the victim of a scam when she attempted to withdraw the \$80,000 she believed she'd earned but was told there were various problems and additional fees she had to pay before she could withdraw the money. Ms H didn't receive the funds she sent or the commission she'd supposedly earned.

Ms H reported the scam to Barclays in November 2024, at the same time as making a complaint via a professional representative. In short, Ms H said Barclays hadn't done enough to protect her from the scam.

Barclays sent a response to Ms H and said that a scam claim hadn't been raised yet and that its fraud team would need to ask her some questions before being able to raise a scam claim. Unhappy with the response, Ms H brought her complaint to our service. After the complaint was referred to this Service, in summary, Barclays said it wasn't the point of loss for the card payments so it wasn't responsible for them, that none of the payments Ms H has disputed were so out of the ordinary to require an intervention and that when it did speak to Ms H, she misled it about the purpose of the payments. Barclays also said it didn't have enough information about the due diligence Ms H carried out and needed more information from her to consider the faster payments under the provisions of the Contingent Reimbursement Model Code ('CRM Code').

An Investigator considered the complaint and didn't recommend that it be upheld. In short, he said the CRM Code didn't apply to any of the payments, Barclays should have been concerned about some of the payments, but if it had intervened it wouldn't have made a difference. Ms H didn't agree with the Investigator's findings and said the payments were out of the ordinary and Barclays hadn't provided adequate interventions and warnings that could have uncovered the scam.

The complaint was reviewed by a second Investigator, and a second assessment was sent – reaching broadly the same outcome but for different reasons. The second Investigator considered that the faster payment transfers were covered by the CRM Code, though the payments to Ms H's own account were not. She reached the conclusion that the card payments weren't unusual enough to require an intervention. For the other payments, the Investigator said Barclays could rely on one of the exceptions to reimbursement under the CRM code. She also said Barclays should have provided Ms H with an Effective Warning at the time of one specific payment, but she didn't think it would have made a material difference in preventing the scam so didn't recommend Barclays reimburse Ms H.

Via her professional representative, Ms H disagreed with the second assessment and provided several reasons why. Because the complaint hasn't been resolved informally, it has been passed to me to make a final decision.

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.

I have summarised this complaint in less detail than the parties involved. I want to stress that no discourtesy is intended by this. If there is a submission I have not addressed, it is not because I have ignored the point. It is simply because my findings focus on what I consider to be the central issues in this complaint.

In deciding what's fair and reasonable, I am required to take into account relevant law and regulations, regulators' rules, guidance and standards, and codes of practice; and, where appropriate, I must also take into account what I consider to have been good industry practice at the time.

Ms H authorised the payments. So in line with the Payment Services Regulations 2017 Ms H is deemed liable for the transactions in the first instance. But she says she has been the victim of an authorised push payment (APP) scam.

Is it appropriate to determine this complaint now?

Barclays didn't fully consider Ms H's fraud claim because she needed to provide it with more information first. But I'm satisfied that Ms H's representative's letter specifically said that Ms H wanted her representative to raise the claim, and appropriate authority was given. I can see that Barclays attempted to contact Ms H around the time it received the claim/complaint letter, but if it needed more information it could have made further attempts to ask Ms H's representatives directly.

Barclays hasn't disputed that Ms H was the victim of an APP scam but also hasn't given an outcome to the claim. Having considered all the evidence I've seen, I'm satisfied that on balance Ms H has been the victim of a scam. So I've gone on to consider whether Barclays should have reimbursed Ms H under the provisions of the CRM Code (for the payments that

fall within the scope of the CRM Code) or reimburse any of her payments for any other reason.

The type of payments Ms H made

While Barclays was signed up to the CRM Code at the time of these payments, the CRM Code does not apply to card payments or payments made to a person's own account. So the first 11 payments Ms H made are not caught by the CRM Code.

The rest were faster payments to an account in the name of a business. There has been some confusion about whether the faster payments were actually peer-to-peer payments in exchange for cryptocurrency. But Ms H's representatives have clarified that these payments were not peer-to-peer payments. Barclays hasn't suggested they were either, and in its response to our service has said that the CRM Code is relevant to those payments. I haven't seen convincing evidence that persuades me on balance that those payments were peer-to-peer payments for cryptocurrency. And as there's no dispute, I've considered whether Barclays should have reimbursed the faster payment transfers under the provisions of the CRM Code.

Ms H's vulnerability and the CRM Code

Ms H has kindly told us about several significant events that happened before and around the time of the scam and that these events had caused her significant emotional and financial stress. Ms H has said she believes these circumstances combined with the ongoing pressure from the scammer impaired her ability to make rational decisions and that she was vulnerable as defined by the CRM Code.

The CRM Code says that a Customer is vulnerable to APP scams, if it would not be reasonable to expect that Customer to have protected themselves, at the time of becoming the victim of an APP scam, against that particular APP scam, to the extent of the impact they suffered.

I have carefully considered what Ms H has said, and I have no doubt her circumstances were difficult and causing her stress and upset at the time. I also accept she was looking to make more money to help with financial concerns, but I don't think Ms H's circumstances at the time of the payments reasonably prevented her from being able to protect herself from being scammed.

I've been able to listen to several calls between Ms H and Barclays, and R, from the time, and review the chats with the scammer. None of the calls or the chats suggest Ms H wasn't able to understand what she was being asked or told by either the bank or the scammer. She was able to formulate her own answers to questions the bank asked and acknowledge the bank's fraud concerns. I appreciate that as the scam progressed Ms H became concerned about losing the money she had already paid, and this was no doubt stressful and a motivator to continue making payments. But based on the information I've reviewed, I'm not persuaded that her circumstances meant she wasn't reasonably able to take any steps to protect herself from this particular scam.

So while I don't doubt the effect Ms H's circumstances had on her at the time, for the reasons above, I don't agree that they meet the CRM Code definition of vulnerability. It follows that I don't think Barclays needs to reimburse Ms H under this particular provision of the CRM Code.

Is Ms H entitled to reimbursement under the CRM Code?

Under the CRM Code, the starting principle is that a firm should reimburse a customer who is the victim of an APP scam (except in limited circumstances).

The CRM code says a Sending Firm (in this case Barclays) may choose not to reimburse a customer if it can establish that the customer made the payment without having a reasonable basis for believing that the payee was the person the Customer was expecting to pay, the payment was for genuine goods or services; and/or the person or business with whom they transacted was legitimate. There are other exceptions outlined in the CRM Code that do not apply to this case.

When assessing whether it can establish these things, Barclays must consider whether they would have had a '*material effect on preventing the APP scam*'.

Reasonable basis for belief

Taking into account all of the circumstances of this case, I don't think Ms H had a reasonable basis for believing the payments were for genuine goods or services; and/or the person or business with whom she transacted was legitimate.

I consider there to have been enough warning signs that ought to have caused Ms H concern from the outset, which she does not appear to have reasonably acknowledged or acted upon. Based on the evidence I've reviewed it seems to me that Ms H took what she was being told by the scammers at face value and doesn't appear to have completed any independent research.

- Ms H was told the job was to help merchants by increasing sales figures and positive reviews of products. Aside from being asked whether Ms H had experience of shopping online, there was no discussion about whether Ms H's skills and experience made her suitable for the role. There was no interview process and Ms H started the supposed job almost immediately with no employment contract or other documentation or processes that would reasonably be expected in a legitimate employment opportunity.
- Although Ms H was able to withdraw a small profit at the very beginning, I think it should have been concerning that Ms H had to pay to perform the tasks she was completing. And fairly quickly she had to pay more and more in order to complete tasks and this was causing her a lot of stress each time. Considering the main purpose of employment is to earn money, I think Ms H reasonably should have questioned why she was having to pay more money simply to fulfil her apparent job role and for products she would not actually be receiving.
- Ms H was repeatedly told to mislead Barclays and her other account provider about the reasons for her payments. I think this should have been concerning from the start and throughout the scam as Ms H sent more funds even though she was aware that both Barclays and R had fraud concerns.
- The base salary, as well as the bonuses and commissions Ms H was told she would receive, for low skilled work and minimal time commitment, were too good to be true.
- The role was to review products that Ms H didn't own and had no experience of, which in itself is dishonest and should reasonably have been questioned.
- Ms H doesn't appear to have completed any independent research into the opportunity, and I think a relatively quick search online about the nature of the role would likely have provided results outlining that this had all the hallmarks of a scam.

So by the time of the faster payments I think there were sufficient red flags that ought to have led Ms H to have acted more cautiously than she did. As such, I think Barclays can fairly rely on one of the exceptions to reimbursement – that Ms H made the payments without a reasonable basis for believing that the payments were for genuine goods or services and/or the person or business with whom she transacted with was legitimate.

Did Barclays meet its standards?

The CRM Code sets out standards that firms are required to meet. Where these are not met, the firm may still be liable to reimburse a victim in part, even where it has been able to establish that an exception to full reimbursement may be fairly applied (as I am satisfied Barclays can establish here).

Those requirements include the provision of what the CRM Code defines as an ‘Effective Warning’ when a firm identifies an APP scam risk in relation to a payment. In short, the CRM Code says that where the firm identifies an APP scam risk it should take reasonable steps to provide their customer with Effective Warnings. It goes on to say that as a minimum, an Effective Warning should be understandable, clear, impactful, timely and specific.

Barclays only needs to provide an Effective Warning when it identifies APP scam risks during a payment journey. Ms H has said that Barclays should have been concerned about several of the faster payment transfers, including the first one where Ms H chose the purpose “friends and family” when the account was a business account.

But based on what Barclays could reasonably have known at the time, I consider the only faster payment that would have particularly stood out as being at risk of being connected to a fraud or scam was a payment of £2,500 on 6 June 2024. I say this because, the other faster payments were not so unusually large or out of character, nor did they follow common patterns associated with scams, such as multiple payments made in quick succession or rapidly increasing payments. And having looked at Ms H’s account activity, it wasn’t uncommon for her to send larger value faster payments. There was also nothing unusual about the recipient that would cause Barclays concern and there was a confirmation of payee match when the payee was setup.

But on 6 June 2024, although the payee had become well established by then, Ms H made two payments of £2,500 within around 10 minutes of each other, and I do think this was unusual compared to her usual account activity. So, I think Barclays should have provided Ms H with an Effective Warning at the time of the second payment of £2,500 on 6 June 2025 – but it didn’t.

However, the CRM Code also says “*The assessment of whether a Firm has met a standard or not should involve consideration of whether compliance with that standard would have had a material effect on preventing the APP scam that took place*”.

I don’t consider that Barclays could reasonably have given a warning that would have likely made a difference in this instance and I don’t think this would have had a material effect on preventing the scam that took place.

I say this because, Ms H spoke to both Barclays and her other account provider, R, several times before the payment on 6 June 2024. Ms H wasn’t truthful with either Barclays or R when both asked her about the purposes of the payments, how she knew the recipients and why she had opened her account with R – despite both Barclays and R explaining that it was important to be honest in her answers.

Ms H also had a very detailed call with R in May 2024, where she was very clearly told about several key features of the scam she was unfortunately falling victim to. Despite Ms H having

experienced all of the features of the scam that R told her about, she acknowledged what she'd been told but assured R that nothing like that was happening and if it were she would say so.

The earlier calls with Barclays and R don't replace the requirement of Barclays to provide Ms H with an Effective Warning on 6 June 2024 or change the fact that it didn't do so. But those calls and her actions following the calls do evidence how Ms H interacted with Barclays, and R, when it did intervene. It also evidences that despite receiving a very clear, timely and specific warning about job task scams from R, Ms H continued to make payments towards the scam despite having experienced all of the elements of the scam that R warned her about. She was also aware of the general risk of fraud, having told both Barclays and R that she had previously been the victim of a scam, and she told the scammer several times that her bank had fraud concerns – but continued to make the payments anyway despite those concerns.

I'm also mindful that Ms H has confirmed she followed the scammer's instructions through each payment journey and each time she received friction from the bank, and has said by the time she spoke to R she was so emotionally invested, stressed and focused on recovering her money that she didn't accept the warning she'd received from R.

So overall, while I accept that Ms H has been the victim of a cruel and sophisticated scam, and I don't blame her for what happened, on balance, I'm not persuaded it would have made a material difference to the success of the scam if Barclays had provided her with an Effective Warning at the point I think it should have done. It follows that Barclays does not need to reimburse Ms H under the provisions of the CRM Code.

Should Barclays have done anything else to prevent the loss?

Outside of the CRM Code, good industry practice requires that regulated firms such as Barclays engage in the monitoring of customer accounts and to be on the lookout for suspicious or out of character transactions with an aim of preventing fraud and protecting customers from financial harm. The Financial Conduct Authority's Consumer Duty was also in force at the time these payments were made, this requires firms to act to deliver good outcomes for consumers including acting to avoid foreseeable harm, for example, by operating adequate systems to detect and prevent fraud.

Barclays was also required to look out for signs of vulnerability. I've already touched on the circumstances Ms H told us about, and I'm sorry to hear about what she was experiencing. However, prior to her making payments to the scammers, I can't see that she made Barclays aware of any vulnerability that required intervention.

Interventions

I've looked closely at all the transactions Ms H made, including the first 12 card payments to her own account, when considering whether Barclays could have done anything else to prevent Ms H's loss. But aside from the one payment already explained above, I don't think any of the other payments should have been viewed by Barclays as highly uncharacteristic, unusual or suspicious enough to warrant an intervention.

This is because, even though they were significant in value, they weren't such large or unusual amounts to suggest they were fraudulent. Though Ms H's account was generally used for every day relatively low value spending, it wasn't unusual for her to send money to her other accounts and to other people and to businesses in the months preceding the scam – including one payment for £4,000 to her own account, and £2,000 to another individual in February 2024. Further, Barclays did speak to Ms H when she first attempted to make

payments to her account with R, and she misled Barclays about the purpose of the payments and why she opened the account with R. Considering Barclays had spoken to Ms H about making payments to her own account, and she regularly transferred sums to and from other accounts in her name, I don't think Barclays needed to be concerned about the card payments she made to her account with R.

As already explained above, I think the only payment Ms H is disputing that should have looked suspicious or indicative of fraud was the second payment of £2,500 on 6 June 2024. I think it should have triggered Barclays' fraud detection systems – prompting it to intervene before releasing the transaction. I am mindful of the fact that the payment occurred after the Consumer Duty came into force. It's my view that a proportionate intervention would have been a scam warning tailored to the likely scam Ms H was at risk of. For example, a warning asking a series of automated questions designed to narrow down the type of scam risk associated with the payment transaction Ms H was making.

But for the same reasons explained above, I'm persuaded Ms H would most likely have proceeded with the payment regardless of Barclays intervening and providing a warning (such as the one described above). And I don't think Barclays could have stopped the scam in its tracks.

Recovery of funds

I've considered whether Barclays did what it could to recover the funds Ms H lost after she reported the matter to it.

I would have expected Barclays to have taken steps to try and recover Ms H's funds promptly after she reported the matter to it, but as I understand it, Barclays didn't reach out to the other bank. But scammers will often move money from their account quickly. The final payment Ms H is disputing here was made in June 2024 but she didn't raise the matter with Barclays until over five months later in November 2024. No evidence has been provided to suggest that any of Ms H's funds remained in the recipient account at the point she raised her claim with Barclays. On balance, I don't think it's likely that any of Ms H's funds would have been recoverable had Barclays attempted to recover them when she first got in touch to report the matter.

Regarding the card payments, the only option Barclays had to recover Ms H's funds was via a Chargeback claim. Chargeback is a voluntary scheme and banks are under no formal obligation to raise a claim and the rules are set by the card scheme.

I would only expect Barclays to have raised a Chargeback if there was a reasonable prospect it would succeed. Unfortunately, Chargeback claims don't cover scams. And because the payments were made to Ms H's own account that she had control of, there wouldn't have been a reasonable prospect of the Chargeback succeeding. So I don't think it was unreasonable that Barclays didn't take any further action at the time.

Summary

I know this outcome will be very disappointing for Ms H but I don't find Barclays is to blame for her losses. I don't find it is liable to refund Ms H under the terms of the CRM Code or for any other reason. In saying this, I want to stress that I am very sorry to hear about what happened to Ms H and I am sorry she has lost out here. She was the victim of a cynical scam designed to defraud her of her money and provide nothing in return. But I can only look at what Barclays was required to do – I have no power to consider the actions of the criminal scammers who were ultimately responsible for Ms H's loss.

Having considered everything very carefully, in my judgment, this is a fair and reasonable outcome in the circumstances of this complaint.

My final decision

For the reasons explained, I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms H to accept or reject my decision before 15 April 2026.

Mike Southgate
Ombudsman