

The complaint

Ms K complains that HSBC UK Bank Plc, trading as first direct ('First Direct'), won't refund the money she lost as a result of what she believes was an 'Authorised Push Payment' ('APP') scam.

Ms K brings her complaint with the assistance of a professional representative. For ease of reading within this final decision, I will refer solely to Ms K in the main.

What happened

The background to this complaint is well known to both parties and has been set out in detail by our Investigator within their view. So, I won't repeat it all in detail here. But in summary, I understand it to be as follows.

Ms K says that she was persuaded to invest with a company that I'll refer to as 'Company V' in my decision. Company V claimed to be a multi-level marketing company that offered customers financial education packages with access to online training on things such as Forex and cryptocurrency trading.

Customers could seemingly choose from a variety of packages ranging from \$50 to \$10,000. Company V told customers that the money spent on packages would be placed into Company V's 'pool' which was then invested in cryptocurrencies, Forex, equities and non-fungible tokens ('NFT's). This meant customers could receive a 2-3% return each week on the amount that they had paid for their training package, and the duration was for 60 weeks. Alongside this, if customers recruited additional people who in turn bought an educational package, they could also earn additional income.

People were required to make payments through cryptocurrency – which would in turn get customers Company V 'points' which could then be used to purchase the training packages.

Ms K was interested in learning new financial skills and was predominantly persuaded to pay for a package with Company V by one of the 'top leaders' / promoters within the UK – whom I'll call Mr J.

Ms K had numerous conversations not only with Mr J but with one of the founders of Company V, whom I'll call Mr M. Ms K also subsequently attended an informal three-day retreat with other members of Company V – which was seemingly paid for by Mr J/ Company V.

Ms K made payments towards a package. She made three payments (totalling £14,600) to Mr J who in turn allocated the equivalent amount of Company V 'points' to her. Ms K also made three smaller payments (totalling £550) to a cryptocurrency account in her own name, which she then sent on to the wallet address provided by Company V.

Customers of Company V ultimately faced issues getting withdrawals and it is now widely accepted that Company V were likely operating a Ponzi / pyramid scheme style scam.

Ms K complained to First Direct advising it should reimburse her under the Lending Standards Board's Contingent Reimbursement Model Code ('CRM Code'). This was a voluntary code that was in force at the time the payments were made and that First Direct was a signatory of. The CRM Code required firms to reimburse customers who had been the victims of APP scams in all but a limited number of circumstances.

First Direct issued a final response in which it declined reimbursing Ms K, so she referred the matter to our service for an independent review.

Our investigation so far

The Investigator who considered this complaint didn't recommend that it be upheld. In summary, she considered the CRM Code didn't apply to any of the payments Ms K had made. And this was because – for the payments Ms K made to Mr J, he had provided her with the 'points'. And she said there was currently nothing to suggest that Mr J was aware that Company V was likely operating a scam. So, she didn't consider Mr J had an intent to defraud Ms K – which was required for the CRM Code to become applicable. And for the payments Ms K made to the cryptocurrency account – as those payments were to an account in her own name, the CRM Code also wasn't applicable as the CRM Code required the payments to go to "*another person*". Our Investigator also thought, given Ms K's belief in things, that any intervention from First Direct wouldn't have prevented the loss nor could it have recovered any funds.

Ms K disagrees and maintains that her complaint about the payments to Mr J, should be upheld under the CRM Code. Ms K also considered that more could have been done to prevent the loss.

As Ms K didn't accept the Investigator's opinion, the complaint has been passed to me for 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.

Ms K's representative has made detailed submissions in support of her complaint and in response to the Investigator's view. I would like to assure Ms K that I've read and considered everything that has been submitted. However, I don't intend to respond in similar detail. I'm aware that I've summarised this complaint briefly, in less detail than has been provided, and in my own words. No discourtesy is intended by this. Instead, I've focussed on what I think is the heart of the matter here. If there's something I've not mentioned, it isn't because I've ignored it. I haven't. I'm satisfied I don't need to comment on every individual point or argument to be able to reach what I think is the right outcome. Our rules allow me to do this. This simply reflects the informal nature of our service as a free alternative to the courts.

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

Where evidence is unclear or in dispute, I reach my findings on the balance of probabilities – in other words on what I consider most likely to have happened based on the evidence available and the surrounding circumstances.

In broad terms, the starting position at law is that a bank is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. But there are circumstances when it might be fair and reasonable for a firm to reimburse a customer even when they have authorised a payment.

Of particular relevance to the question of what is fair and reasonable in this case is the CRM Code, which First Direct had signed up to.

The CRM Code doesn't apply to all APP payments which ultimately result in a loss for the customer. It only covers situations where the payment meets its definition of an APP scam.

The relevant definition for this case would be that Ms K transferred funds to another person for what she believed was a legitimate purpose, but which was in fact fraudulent. In this case, the first three payments Ms K made, were to Mr J and not Company V direct. So, Ms K did pay another person.

To decide whether Ms K is the victim of an APP scam as defined in the CRM Code I have considered:

- The purpose of the payments and whether Ms K thought this purpose was legitimate.
- The purpose the recipient (here that is Mr J) had in mind at the time of the payments, and whether this broadly aligned with what Ms K understood to have been the purpose of the payments.
- Whether there was a significant difference in these purposes, and if so, whether it could be said this was as a result of dishonest deception.

I've considered the evidence available, but I can't fairly conclude that Ms K has been the victim of a scam in line with the required definition. This means the CRM Code doesn't apply to the payments she made to Mr J and so First Direct isn't required to reimburse her under it.

Our Investigator covered why they considered the payment purpose Ms K had in mind, and the purpose in which the recipient (Mr J) had, matched. I'm in agreement with them that this was the case, I'll explain why.

While it's widely accepted that Company V were operating a scam, I've not currently seen anything to suggest that Mr J, who was a promoter or 'top leader' for Company V, was aware and was more likely than not complicit. In the absence of any further evidence, and based on the balance of probabilities, it is just as equally likely that Mr J was a victim of Company V and was himself trying to recruit additional people to purchase training packages which would obtain him additional income. Here, Mr J had 'points' and he sent those points to Ms K, with Ms K transferring him the required funds.

So, if my starting position – based on having no evidence to the contrary – is that Mr J wasn't complicit in the scam, then as Ms K wanted to obtain Company V points and Mr J allocated/sold her his points – then their purposes aligned. For all intents and purposes, they were genuine payments, to the person Ms K was intending to pay and that Mr J's intention for receiving the payments was the same as Ms K's purpose for making them. So, whilst the payments were made and were ultimately in relation to Company V, Ms K's payments to Mr J don't meet the criteria for the CRM Code to apply.

So, I can't agree First Direct was wrong in not reimbursing Ms K under the provisions of the CRM Code for the payments she made to Mr J.

This also means I'm unable to ask First Direct to reimburse Ms K on the basis that she was vulnerable at the time the payments were made. When the CRM Code applies, a customer can be reimbursed if they are vulnerable – even when an exception to reimbursement applies. But as that's not the case here and the CRM Code doesn't apply, I won't be asking First Direct to reimburse Ms K.

If material new evidence comes to light at a later date that strongly indicates Mr J was complicit in the scam orchestrated by Company V, Ms K can ask First Direct to reconsider her fraud claim for those payments she made to Mr J.

I've gone on to think about whether First Direct should be held responsible for Ms K's loss for any other reason – including the payment she made to her own cryptocurrency account (which also aren't caught by the provisions of the CRM Code as Ms K didn't pay *another person*).

As explained earlier, First Direct is expected to process payments and withdrawals that its customer authorises it to make, but First Direct should have also been on the look-out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). And, in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment.

I think First Direct ought to have had some concerns, and its interventions/questioning could have gone further than they did. But this in and of itself, isn't enough for me to say that First Direct should refund Ms K the money she lost. Although it's arguable that First Direct could have done more than it did, I also need to be persuaded that any further proportionate intervention/questioning would have made a difference and prevented the payments from being made. Of course I can't know for sure what would have happened, so I have to base my findings on the balance of probabilities – that is, what I think is more likely than not to have happened, taking into account what I know.

In doing so, I am mindful of Ms K's belief in things and that she considered Company V were legitimate, despite there being some quite obvious concerns and negative information about Company V online at the time. Ms K has said she carried out research into Company V and therefore she wasn't seemingly put off by the negative reviews. Ms K also had multiple online meetings and was being mentored by Mr J who was one of the leading promoters within the UK. I can also see that Ms K was a part of online meetings where Mr M (one of the founders of Company V) was present. Ms K has said she questioned the reviews and Mr M seemingly provided sufficient answers that assured her everything was legitimate.

In short, what this means, is that despite a considerable amount of negative information publicly available about Company V, Ms K was satisfied enough to proceed in light of that – and that was based on her interactions with Mr J, and Mr M. So, I'm not as persuaded as I would need to be, to say that had First Direct carried out some additional checks that it would have had a material effect and prevented her from making the payments. Nor do I find that she would have likely heeded any warnings First Direct might have put forward, such as her belief in things at the time.

Overall, with all things considered and given the circumstances, I don't think First Direct can fairly be held responsible for Ms K's loss, and I don't think, in the individual circumstances of this case, the evidence supports that it would likely have been able to prevent Ms K from making these payments either.

I've thought about whether there was any opportunity for First Direct to have recovered the money Ms K had lost, once it was made aware of the scam. There was no obligation for First Direct to try and recover the payments Ms K made to Mr J, as the payments aren't covered by the provisions of the CRM Code. And with the payments Ms K made to a cryptocurrency account in her own name, given the funds had been exchanged into cryptocurrency and then moved on to accounts controlled by the fraudsters, I don't think there was any opportunity or prospect of First Direct being able to recover any of the money.

I don't intend any comments or findings I've made in this decision to downplay or diminish the impact this scam has had on Ms K. It's very unfortunate she has lost this money in this way, and I understand the whole experience has been deeply upsetting and I do have a great deal of sympathy for her. But in the circumstances, having carefully considered everything, the payments Ms K made aren't covered by the provisions of the CRM Code, and I don't find First Direct could have reasonably prevented Ms K's loss here. Neither do I find there were any other failings on First Direct's part that would lead me to uphold this complaint.

My final decision

For the reasons given above, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms K to accept or reject my decision before 12 December 2025.

Matthew Horner
Ombudsman