DRN-4562810

## The complaint

A company - F, complains that The Co-operative Bank Plc (Co-Op Bank) won't refund the money it lost as a result of a scam.

The complaint is brought on F's behalf by its director, Mr L.

## What happened

In late July 2023, Mr L was looking to buy a laptop for an employee of F. After experiencing issues with a laptop he'd purchased via a well-known selling platform (that I'll call E) some weeks prior, he turned to a social media marketplace (that I'll call M). He found a seller based locally who was selling a used laptop for £400. He contacted the seller via messenger on M, but the seller explained he was currently on holiday elsewhere in the UK until the end of September 2023. He offered Mr L the option of collecting the laptop from where the seller was on holiday, but Mr L explained this would be a journey of four to five hours. The seller instead agreed to post the laptop to Mr L for an upfront payment of £200, and once Mr L received the laptop and confirmed it was as described, he could pay the other £200. He made a bank transfer to an account he thought belonged to the seller's partner, on 14 July 2023. The laptop was due to be sent directly to F's employee via tracked and signed-for delivery.

Once Mr L paid the £200, the seller explained their partner had been spooked by concerns raised by members of the postal staff about posting a high value item like a laptop without having been paid in full. The seller explained the laptop was being held by the postal staff until the full payment had been received. Mr L expressed concern that this was not what they had agreed and so the seller offered Mr L a refund. But Mr L had already been through a dispute process following the issues with the first laptop he'd bought via E, and he didn't want to do that again. As he needed the laptop, he proceeded to pay the second payment of £200 on 15 July 2023. However, the seller didn't provide the tracking as agreed and F's employee confirmed they did not receive the laptop, which was due to arrive by 17 July 2023.

Mr L contacted Co-Op Bank at around 17:53 on 17 July 2023 to report that F had been scammed. Co-Op Bank contacted the bank that received F's funds. It says it did this around 08:56 on 18 July 2023, but it confirmed no funds remained for recovery and the receiving bank didn't accept liability for F's loss.

Co-Op Bank declined to refund F under the Contingent Reimbursement Model (CRM) Code, of which it's a signatory. The CRM Code sets out that Co-Op Bank should refund victims of authorised push payment (APP) scams (like F), in all but a limited number of circumstances. Co-Op Bank said two exceptions to reimbursement applied. It said:

- F made the payment without a reasonable basis for believing that; (i) the payee was the person it was expecting to pay, (ii) the payment was for genuine goods or services, and/or (iii) the person or business F paid was legitimate.
- F did not follow its own internal procedures for approval of payments, and

Co-Op Bank considered that those procedures would have been effective in preventing the scam.

Mr L complained on behalf of F to Co-Op Bank, but its position remained the same.

Unhappy with this response, he referred F's complaint to this service, but our Investigator didn't uphold it. They firstly considered whether F's dispute had arisen from a civil dispute, rather than a scam. This was relevant because only scams are covered by the provisions of the CRM Code. But they were satisfied there were elements of what happened pointing to it being a scam and so the CRM Code applied. But they said Co-Op Bank had fairly established that under the CRM Code, F didn't have a reasonable basis for believing that the payment was for genuine goods or services, and/or the person F transacted with was legitimate. They didn't agree there was any other reason why Co-Op Bank would be obliged to refund F as it met its standards under the CRM Code. This is because they didn't consider it was necessary for Co-Op Bank to provide an Effective Warning, nor did they think Co-Op Bank could have recovered F's funds.

Mr L didn't agree with our Investigator's recommendations. He said the price of the laptop wasn't too good to be true and he did conduct research into the laptop he was buying from M.

Our investigator wrote to Co-Op Bank in advance of my final decision. She asked it whether it would consider refunding 50% of the payments F made, because Mr L had exchanged identification with the seller and saw a video of the laptop. Co-Op Bank decided not to make an offer to resolve the complaint. However, it did clarify that when it said F did not follow its own internal procedures for approval of payments, it meant it didn't conduct sufficient due diligence before making the payments and it was not aware of any internal procedures for approval of payments that F had in place. Our Investigator subsequently reiterated to Mr L that her recommendation was unchanged from the view she sent to both parties on 9 November 2023 - she did not think that the complaint should be upheld.

As no agreement could be reached, this case was passed to me for a decision to be issued.

**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.

When reaching my decision, I'm required to take into account relevant: law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to be good industry practice at the time.

Having done so, I agree with the outcome issued by our Investigator and broadly for the same reasons. I'll explain why.

I appreciate Mr L feels strongly that Co-Op Bank ought to refund F because it has been scammed. I'm sorry to say that faster payments, like the two F has disputed, don't attract the same consumer protections as payments made by plastic card. So whilst he was able to raise a dispute for the card payment he made to E and successfully received a refund, such protections are reserved for card payments only.

Mr L acknowledges he carried out the transactions in dispute, albeit he was tricked into doing so. Under the relevant regulations, namely the Payment Services Regulations 2017 (PSR 2017), F is responsible for transactions he has authorised. But where the customer

has fallen victim to an APP scam, the provisions of the CRM Code could be relevant and Co-Op Bank could, in some cases, be held liable for a customer's losses.

Is it a scam or a civil dispute?

For the CRM Code to be relevant, F would have to have been the victim of an APP scam, which is defined in the CRM Code as:

> *...a transfer of funds executed across Faster Payments…where:*
>
> *(i) The Customer intended to transfer funds to another person, but was instead deceived into transferring the funds to a different person; or*
>
> *(ii) The Customer transferred funds to another person for what they believed were legitimate purposes but which were in fact fraudulent*

As F intended to transfer the funds to the seller, I'm satisfied (i) is not relevant here. In order for the second provision to apply, I'd need to be reasonably satisfied from the evidence that the seller intended to deceive F by acting fraudulently.

Co-Op Bank says that in a call on 6 October 2023, Mr L expressly confirmed that he had in fact received the laptop in exchange for the two payments he'd made for £200. This is a clear distinction from the one off payment he made for the first laptop he had issues with, which is not the subject of this complaint. This would point to this dispute being a civil matter and not a scam, as Mr L confirmed in this call that he had received the laptop.

Mr L disputes this and has since confirmed to our Investigator that he did not receive any laptop from the seller on M in respect of the two £200 transfers in dispute.

I've listened to the call Co-Op Bank has referred to, dated 6 October 2023. In this call, Mr L confirmed he reported a scam for a '£400 laptop' and he has since received the laptop and it is broken. When asked in the call which payments this refers to, he confirms it refers to 'two £200 payments' made in July. So I am satisfied Mr L was referring to the laptop he'd bought via M and not the laptop he'd bought via E. He also said in this call, that the bank had previously advised him on a call that if he received a laptop and it was broken that he'd receive a refund.

Co-Op Bank has suggested Mr L was trying to raise F's claim again, in a different way, in order to get the same outcome as when he disputed the payment he'd made via E. I've carefully considered whether I think Mr L did receive a faulty laptop via M, in which case his dispute would be the subject of a civil matter and not something Co-Op Bank would have any liability for, or whether, like Co-Op Bank suggested, he had not received the laptop but was attempting to obtain a refund in a different way. Having done so, I think it's more likely than not the latter of the two.

Mr L was quite insistent in this phone call that F should get a refund because it had been refunded in the same way previously when he received a faulty laptop, and because Co-Op Bank had told him on a call previously that he'd get a refund if he received a faulty laptop.
It's worth me highlighting that the two claims are different, and Co-Op Bank would have no obligation to uphold the second claim just because it upheld the first. Nor would it be bound by anything it may have said during a phone call, about a situation which had not yet occurred. But, in sentiment, it does appear that Mr L was attempting to draw similarities between the claim raised initially for the payment to E, and the payments he made to the fraudster from M, in order to achieve the same outcome.

I also think, from the evidence supplied by Mr L, that the correspondence between him and the scammer carried many hallmarks of a classic purchase scam. The seller was said to be located locally, but once contact was made, they were hours away – making a face to face sale much less appealing. The price of the item was below what I'd expect it to be, considering the make and model of the laptop being purchased. And Mr L sent the funds to a third party account which wasn't in the name of the seller. I've contacted the bank Mr L sent F's funds to and they confirmed they treated F's report against their customer as a valid scam claim.

On balance, I'm satisfied F likely did fall victim to a scam and this claim is not the subject of a civil matter. Therefore I think the CRM Code is a relevant consideration of F's complaint.

Has Co-Op Bank fairly established an exception to reimbursement applies?

As I've already set out, Co-Op Bank is a signatory of the CRM Code. The starting position under the CRM Code is that Co-Op Bank ought to refund F, unless it can establish an exception to reimbursement applies. Such exceptions to reimbursement include (as far as is relevant to this complaint) that F:

- Made the payment without 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.
- Did not follow its own internal procedures for approval of payments, and those procedures would have been effective in preventing the APP scam;

In this case, I think that Co-Op Bank has fairly established that F lacked a reasonable basis for believing that the person or business with whom it transacted was legitimate. I know this might be disappointing for Mr L, so I'll explain why I've reached this decision.

I agree with our Investigator that the laptop was being sold for seemingly less than it might be worth. Mr L paid £400 in total for the laptop. The messages between Mr L and the fraudster suggest this didn't include a postage fee, and Mr L says he can't recall what was discussed about postage. Mr L also says the laptop was worth £600 but the seller *'wanted it to go to a good home'* so they agreed to reduce the price to £400. But it seems unusual for a seller to reduce the price of a laptop it was selling by such a significant amount, for sentimental reasons.

Mr L says he paid £474.99 for a laptop via E, which he received in working condition (albeit he experienced some issues with this). So he doesn't think the price he paid the fraudster was too good to be true. He says he's bought trainers via E before which were half the retail price, so he did not find the price to be unusual. He also says it's well-known that M offers items at a cheaper price than E.

However, the laptop Mr L bought via E was listed for £549 and he paid less than this using a promotional offer from E. Also, the laptop Mr L bought from E was a less superior model than the one he bought via M. So I can understand why this might have been sold for a lower price than what our Investigator said the laptop from F was worth.

Mr L also provided a number of screenshots of ads on E for similar laptops being sold for a range of prices, some below £400. But such ads are quite often listed by private sellers on marketplaces like E and M. As Mr L has experienced, such ads can be fraudulent and so the price of these items are not always reliable. But I have also reviewed similar listings on E, but for users with 100% positive feedback as I find these to be more reliable listings. In doing so, I've found a price range of £650 to £1,200. And I've considered advertised laptops from

reputable merchants, and for a refurbished laptop of the same spec, the price is £721. I therefore think Mr L ought to have questioned why the seller agreed to sell the laptop for just £400. I can see why this low price likely would have enticed Mr L. But this can also be an indicator that something is not quite right about the seller or proposed deal being offered. I think the price was enough to have caused Mr L serious concerns about the legitimacy of the sale and in turn, the legitimacy of the seller, particularly as he'd not seen the laptop in person.

I do appreciate Mr L took some steps to verify the seller. He checked the seller's profile, and they exchanged electronic copies of their driver's licence. Albeit the seller did not provide his own and instead sent a copy of his partner's driving licence as F would supposedly be sending the funds to their account. This was done as a show of faith, and I can see why it might have provided Mr L with some reassurances, but it did little to prove that the seller was genuine, or that they genuinely had the item for sale in their possession.

Furthermore, there were repeated inconsistencies in the seller's story. The ad suggested he was local to Mr L, and this is one of the things which initially attracted Mr L to the seller's listing. However once contact was made, the seller claimed to be on holiday until the end of September and just so happened to have the item with him around five hours away from Mr L, making it highly unlikely he'd go to see the item in person. The seller claimed he was going to the post office which closed at 19:00. He messaged Mr L from within the post office at 19:39 and said it was due to close in around 14 minutes. He also said he'd only post the laptop if postage fees were covered, but he later said they could sort it out after the laptop was received. Whilst some of these might be smaller inconsistencies than others, in my opinion, they build a picture of the seller's untrustworthiness.

What's more, it's clear throughout Mr L's contact with the fraudster that he had an awareness of the risks of using platforms such as M. He made comments such as *'I'm losing faith with M. I've lost a fair amount of cash from people on here',* and *'I wanted to check it personally before sending money this site has caused me problems before',* and *'That's my point M is proper dodgy'*. He said all of these things before he made any payments to the fraudster. Mr L confirmed he said this because he'd had instances on M where conversations had led to nothing, and he had lost money buying a different item before via M. And he confirmed he had been scammed via M before. I therefore think he ought to have been more receptive to the red flags which were apparent at the time, given these concerns and negative experiences he'd already had with M.

Turning to the second payment, I think by this point Mr L ought to have had serious concerns about what he was being told by the seller. They had agreed he would pay £200 up front and £200 once F's employee received the laptop. But the seller then refused to send the laptop to F's employee until Mr L paid the second payment. Whilst I do agree the postal staff could have plausibly expressed concern about someone posting an item that hadn't been paid for in full, (and in turn I also question why Mr L thought it likely the seller would post an item he hadn't paid for in full), I find it very unlikely that the postal staff would hold the parcel to ransom until full payment had been received by the seller. The messages between Mr L and the fraudster show Mr L was unhappy with this request and seemed to have concerns about making a further payment. For example, he said *'If anything I'm the one who should be scared I'm paying for a laptop I'll never see'.* So, it's unclear why he did in fact proceed to pay more.

Taking these things into account, I'm afraid that I find F lacked a reasonable basis for believing that the payment was for genuine goods or services or that the person with whom it transacted was legitimate. Therefore under the CRM Code, F can be held at least partially liable for its loss.

Did Co-Op Bank meet the standards for firms under the CRM Code?

Co-Op Bank also has standards under the CRM Code it's expected to meet as a firm. Failure to do so in relation to a particular payment, or series of payments, could mean it's responsible for partially reimbursing its customer.

The CRM Code requires a firm to provide an Effective Warning where it identifies an APP scam risk in a payment journey. Co-Op Bank has said it presented Mr L with a warning when he made the payments, although it's not been clear on whether it considers this to have been an Effective Warning. However, I'm not persuaded there was enough going on for Co-Op Bank to have identified a scam risk when Mr L made the payments. I say this because the payments were unremarkable in value and nature compared to F's account activity and not out of line from what you might expect to see on a business bank account. So, there was no requirement for Co-Op Bank to provide F with an Effective Warning.

Mr L also says he called Co-Op Bank on 14 July 2023 and in this call, he was given assurances that should he not receive the laptop, he'd get his money back. I've listened to this call and no such comments were made by Co-Op Bank. Nor was there any information revealed in this call about the purpose of the payments. This call was predominantly focused on the technical issues Mr L faced with his online banking. Mr L has since told our service he can't be sure whether this was said in regard to the payment he'd made to E or to the fraudster. But overall, I'm satisfied Co-Op Bank did not miss an opportunity to warn F against the payments it was making.

*Recovery of funds*

I've considered whether Co-Op Bank took appropriate and timely steps to notify the receiving bank of F's claim, in line with its expectations under the CRM Code. I'd have expected Co-Op Bank to contact the receiving bank immediately (or within an hour) from when Mr L reported it, in line with the Best Practice Standards for recovery of funds.

Based on what I've seen, Co-Op Bank didn't contact the receiving bank as quickly as I'd have expected it to, however I'm satisfied this didn't impact F's chances of recovering its funds. I say this because I've received evidence from the bank Mr L sent F's funds to, showing the funds had been removed in full by 15 July 2023, which was before he reported the scam to Co-Op Bank. So despite the delays to Co-Op Bank contacting the receiving bank, this had no impact on the amount available for recovery and so Co-Op Bank would have no liability under the CRM Code.

## My final decision

For the reasons I've explained, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask F to accept or reject my decision before 29 March 2024.
Meghan Gilligan
**Ombudsman**