DRN-4577081

The complaint

Mrs M complains that The Co-operative Bank plc ('Co-op') won't refund the money she lost when she fell victim to a scam.

What happened

Mrs M says that in February 2023 her laptop was making an awful noise and she was unable to get it to stop. A number appeared on her screen, and she rang it to get some help. Mrs M then spoke to two individuals who said they were from the National Crime Agency (NCA)/Action Fraud. They stopped the noise and told Mrs M her identity had been stolen and her account hacked. Mrs M was asked to help to catch criminals by transferring £2,000 to a hacker's account so that the money could be traced. Mrs M was assured that her funds would be reimbursed.

Mrs M was told not to tell anyone about what she was being asked to do and to lie to her bank about the reason for the transaction. She was given a cover story to use if Co-op asked her any questions.

On 20 February 2023 Mrs M made the £2,000 transfer. Co-op blocked the transaction and had a conversation with Mrs M about it. During the call, Mrs M explained that she'd like to pay a garden designer and the following points were covered:

- Mrs M was asked to be honest with Co-op to help protect her from being a victim of fraud and told that if the transaction turned out to be fraudulent, she wouldn't be able to get it back.
- Mrs M was asked if there was anything different or unusual on a personal level that might impact her desire to make the payment. She advised there wasn't.
- The Co-op fraud advisor told Mrs M that some people are tricked into making payments and Co-op wanted to check that wasn't happening to Mrs M. She was asked if she'd been told to lie to Co-op or been coached on what to say. Mrs M said "no".
- Mrs M was asked if she'd been told to move her money to an account that was safe. The advisor went on to say that the bank would never ask her to do that and that if she been told to lie to the bank or coached this would be fraud.
- The advisor covered advice about email intercept scams, whether Mrs M had been pressured to make the payment, the steps she had taken to ensure the recipient was genuine, why the payment wasn't being made by card and whether she had any doubts. Mrs M was also asked to confirm why she was happy to make the payment and what would happen if it turned out to be fraudulent.

Mrs M has explained that one of two people who said they were from Action Fraud then called her daily. They were caring and kind in the calls and built a relationship with her. After the first payment had been made Mrs M was asked to make further payments to help to catch other criminals. Mrs M made two further transactions as requested – one for £9,800 on 10 March 2023 and one for £9,700 on 13 March 2023. Both of these transactions were to the same payee. Both transactions were made via telephone banking as Mrs M didn't use internet banking.

In the call on 10 March 2023 the advisor covered very similar questions and advice as in the previous call, so I won't repeat the information here. This time, Mrs M said that she couldn't get out much and was transferring funds to buy white goods to re-do her kitchen that the lady she was paying had sourced. Mrs M said that the recipient was a friend of the family who was helping her and that her family obtained the payment details and confirmed them with the recipient. Again, Mrs M was asked to confirm why she was happy to make the payment.

Mrs M also used telephone banking to make the final payment on 13 March 2023. She said she was making a second payment to the same payee as before (on 10 March) but this time the payment was to refurbish the house and garden, including buying a new bed and sofa. Mrs M was given the same scam advice as in both previous calls and was asked questions about the transaction and the person she was paying. She stuck to her cover story and didn't admit that she had been advised to lie to her bank when asked.

At a family gathering Mrs M told family members what had happened and was advised she was the victim of a scam. She called Co-op to report the scam on 5 May 2023. Even at this stage Mrs M wasn't sure she really was the victim of a scam.

Co-op assessed Mrs M's complaint under the Lending Standards Board's Contingent Reimbursement Model Code (CRM Code) and said it couldn't refund her. It said that it met the standards expected by providing an effective warning and that it could rely on an exception to reimbursement. This was because Mrs M took what she was told at face value and didn't have a reasonable basis for believing she was making a legitimate payment.

Mrs M was unhappy with Co-op's decision and brought a complaint to this service. She said Co-op hadn't taken into account all the circumstances at the time. She wasn't in the right frame of mind because she was unwell, and on the day after the first payment a dog she had been looking after died and she attended the funeral of a dear friend two days later.

Since Mrs M's complaint has been brought to this service Co-op has been able to recover the initial £2,000 transaction which has now been credited to Mrs M's account.

Our investigation so far

The investigator who considered this complaint recommended that it be upheld. He thought Mrs M was vulnerable to the scam she fell victim to. Even if she wasn't, the investigator said that Co-op couldn't fairly rely on any of the exceptions to reimbursement in the CRM Code, so Mrs M should be reimbursed in full.

Mrs M agreed with the investigator's findings, but Co-op did not, so the complaint has been passed to me to decide. In summary, it said:

- The investigator's conclusion that Mrs M was vulnerable was based on assumption rather than fact. During its fraud investigation it didn't come across any evidence that Mrs M was vulnerable and nothing in the investigator's view changed that.
- The warning provided to Mrs M was effective. It specifically mentioned the police and the NCA is a law enforcement agency; gave examples of types of scams and said fraudsters pose as trusted organisations; asked if she'd been told to lie to her bank and if she'd been coached; to confirm her understanding of what would happen if it turned out to be a scam and encouraged her to reflect on the warnings she had been given.

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.

In deciding what's fair and reasonable in all the circumstances of a complaint, 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 be good industry practice at the time.

The starting position under the relevant regulations, the Payment Services Regulations 2017 ("PSR 2017") and, for transactions earlier than 13 January 2018, the Payment Services Regulations 2009 ("PSR 2009"), as well as under the terms and conditions of this account is that the account holder is responsible for transactions they've authorised themselves, even those carried out under deception.

Co-op is also a signatory to the Lending Standards Board's Contingent Reimbursement Model ("CRM Code"), a voluntary code which requires its signatories to reimburse victims of APP scams in all but a limited number of circumstances. The CRM Code requires a firm to refund customers who are vulnerable to APP scams, regardless of whether any exception to reimbursement might otherwise apply. Under the CRM Code 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 victim of an APP scam, against that particular APP scam, to the extent of the impact they suffered*.'

So, the first point I've considered is whether Mrs M was vulnerable at the time she fell victim to the scam.

The Lending Standards Board in its September 2022 review of adherence to the CRM Code expressed concern about the fact identification of customers vulnerable to scams isn't consistently achieved across the industry. I've listened to the two calls Mrs M had with Co-op staff on the day she reported the scam and note there was no discussion whatsoever around potential vulnerability, even though Mrs M said in the first call that she was unwell at the time. This is particularly concerning given Mrs M's age when the scam happened.

R2(3)a of the CRM Code says:

"*All Customers can be vulnerable to APP scams and vulnerability is dynamic. The reasons for dynamics of vulnerability may include: the personal circumstances of the Customer; the timing and nature of the APP scam itself; the capacity the Customer had to protect themselves; and the impact of the APP scam on that Customer*."

Mrs M has explained that:

- She was unwell at the time of the scam with a cough that prevented her from sleeping. I note in the call when she transferred £2,000 she was hoarse and didn't sound well. I think an illness like this can have quite an impact on someone Mrs M's age.
- A few days after the first payment was made Mrs M had attended the funeral of a "*dear friend*".
- A dog Mrs M cared for had just died.

Mrs M has said that these factors meant that she wasn't in the right frame of mind to deal with everything.

I think this is a much more finely balanced case, but it would be fair to say that Mrs M was vulnerable at the time she made the first payment of £2,000 and I accept there was pressure on her at the time. This transaction has been returned to Mrs M though. After this, I consider the factors Mrs M has pointed to likely played a role in what happened, but I'm not persuaded she was unable to protect herself from the scam she fell victim to. The second two transactions were made weeks after the first. In her call with Co-op when she made the payment on 10 March Mrs M apologised that her voice wasn't good but said that she was otherwise fine. And she was able to create a detailed cover story and stick to it. So I'm not persuaded Mrs M was unable to protect herself from the scam she fell victim to.

I've gone on to consider Mrs M's claim under the remaining provisions of the CRM Code. The CRM Code requires firms to reimburse victims of APP scams like this one unless it can

establish that it can rely on one of the listed exceptions set out in it. Under the CRM Code, a bank may choose not to reimburse a customer if it can establish that:

- The customer made payments 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.
- The customer ignored what the CRM Code refers to as an "Effective Warning" by failing to take appropriate action in response to such an effective warning.

There are other exceptions in the CRM Code that aren't relevant to this case.

I've thought carefully about whether Mrs M had a reasonable basis for believing she was speaking to and helping the NCA. In determining this the CRM Code says that I should take into account all the circumstances at the time of the payment, "*in particular the characteristics of the Customer and the complexity and sophistication of the APP scam*".

I've thought about the matter carefully and think it's finely balanced but, overall, I consider Mrs M's belief that she was making payments to help to catch a fraudster was reasonably held taking into account her characteristics.

In considering whether Mrs M had a reasonable basis for belief when she made the second and third transactions, I've thought about the points she has raised in respect of vulnerability and the following points:

- The scammers called Mrs M most days and were caring in the calls. They built trust and preyed on her isolation. In a letter to this service Mrs M said, "*When all of this ended and no calls came, I felt, at first, bereft, I was so used to talking to them*". I consider this is a significant point in this case and that the scammers made Mrs M believe they genuinely cared for her wellbeing at a time when illness and other factors made her low and less able to recognise what was happening. The other things going on in Mrs M's life at the time made her particularly open to persuasion.
- She was 80 at the time of the scam and wasn't a confident internet user which is why Mrs M didn't use internet banking. This meant she was less able to protect herself in terms of investigating what the scammers told her.

It's also clear to me that Mrs M believed that she was helping to catch a fraudster. Even when she reported what happened to Co-op after speaking to her family Mrs M still wasn't convinced that she was the victim of a scam.

Overall, while I accept this is quite a finely balanced point and not everyone would have followed the fraudsters' instructions in the way that Mrs M did, the test I need to consider is whether in all the circumstances and taking into account Mrs M's circumstances and characteristics, she held a reasonable basis for believing that the caller was legitimate. I think she did.

I've gone on to consider whether Mrs M ignored an effective warning by failing to take appropriate steps in response to it.

For Co-op to rely on this exception to reimbursement I'd need to be satisfied that Co-op provided an effective warning and, if it did, that Mrs M ignored the effective warning by failing to take appropriate action in response to it, and that taking appropriate action would have had a material effect on preventing Mrs M from falling victim to this scam.

I don't consider the warning provided to Mrs M met the minimum requirements of an effective warning in the CRM Code. Mrs M was asked if she had been asked to move money by someone claiming to be the police or the bank and was told that the police or bank won't ask her to do that. But Mrs M wasn't being asked to move funds by the police or a bank. In any event, I am mindful that Mrs M was coached to provide incorrect answers to her bank

and genuinely thought she was helping to catch criminals, so I'm not persuaded she acted unreasonably in moving past the warnings she was given.

Overall, I'm not satisfied Co-op has demonstrated that it can fairly and reasonably rely on an exception to reimbursement, so Co-op should reimburse the second and third transactions.

My final decision

For the reasons stated, I uphold this complaint and require The Co-operative Bank plc to:

- Refund £19,500; and
- Pay interest on the above amount at the rate of 8% simple per year from the date The Co-operative Bank plc decided not to reimburse her until the date of settlement.

If The Co-operative Bank plc considers that it's required by HM Revenue & Customs to deduct income tax from that interest, it should tell Mrs M how much it has taken off. It should also give Mrs M a tax deduction certificate if she asks for one, so she can reclaim the tax from HM Revenue & Customs if appropriate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs M to accept or reject my decision before 13 May 2024.

Jay Hadfield
Ombudsman