DRN-4517697

Complaint

Mrs H is unhappy that Metro Bank PLC hasn't reimbursed her after she fell victim to an investment scam.

Background

In June 2022, Mrs H received a call from a man who claimed to be an employee of a business specialising in cryptocurrencies. He told her that an e-wallet which was under her control had a balance of over £50,000 waiting for her to withdraw. Unfortunately, the caller wasn't a legitimate employee of a cryptocurrency business, but a fraudster.

She had made a small investment in cryptocurrency several months earlier of around £500. The business to which she'd made that payment wasn't (and didn't purport to be) the same business that contacted her in respect of her £50,000 that was ready for withdrawal. However, Mrs H assumed that there was a connection between the two. She hadn't looked at her genuine cryptocurrency account for some months but didn't go back to check what the balance was.

There then followed a series of interactions between Mrs H and different individuals who all claimed to be assisting her with accessing her £50,000. She was told that each payment was a legal or technical necessity to enable her to get access to her money. Some were described as fees and charges, others as "collateral" that would be returned to her once the transaction concluded.

In total, Mrs H transferred over £100,000 in around one month. A detailed account of the circumstances that led to each payment was set out in the Investigator's view and so I don't think it's necessary to repeat that description here. However, it is worth setting out how Mrs H responded when Metro and two other banks involved in the scam spoke to her about the payments.

She spoke to Metro Bank on 30 June and 7 July to discuss payments that she was making. In the second of those calls, she was asked the purpose of the payment. She said it was a personal investment.

On 6 July, she spoke with a different bank and was asked about a £3,000 payment she was intending to make. She told them that she was paying a fee for a training course. In her first conversation with an employee of that bank, she was asked whether the payment was for cryptocurrency. Mrs H responded *"No, no. It's cash. I'm trying to buy something."* In a later call, she was again asked about the purpose of the payment, and she said *"It's just one of the training companies I'm working with. I'm planning to join a course for nutritional therapy."*

Once Mrs H realised that she'd fallen victim to a scam, she notified Metro. It looked into things but didn't agree to refund her losses. It argued that it had provided an 'Effective Warning' prior to her making the payments to the scammer and that this should have made her think twice before proceeding. It also said it had done everything it could to recover Mrs H's funds from the receiving account. Unfortunately, they were moved out of that account promptly and so no recovery was possible.

Mrs H wasn't happy with the response she'd received from Metro Bank and so she referred her complaint to this service. It was looked at by an Investigator who upheld it in part. The Investigator noted that good industry practice required Metro to be on the lookout for out of character activity on Mrs H's account that might have been an indication that there was a risk of financial harm due to fraud.

She thought that Metro ought to have intervened in connection with the 8th payment Mrs H made – a payment for £11,000 on 7 July. She accepted that, given the way Mrs H had responded when another bank asked her about other payments, she was unlikely to have answered questions from Metro honestly. However, she concluded that the activity on her Metro account was so out of character that, even if she weren't forthcoming with information about the purpose of the payment when questioned, it shouldn't have accepted her first answer to its questions. The risk was too stark.

Metro disagreed with the Investigator's view and so the complaint was passed to me to consider and come to a final decision.

Findings

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

I issued my provisional findings on this complaint on 15 November 2023. I wrote:

> *In broad terms, the starting position at law is that a firm is expected to process payments and withdrawals that a customer authorises, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account.*
>
> *However, that isn't the end of the story. Good industry practice required that Metro be on the lookout for payments that were out of character or unusual to the extent that they might have indicated a fraud risk. On spotting such a payment, I'd expect it to intervene in a manner proportionate to the risk identified.*
>
> *Metro is also a signatory to the Lending Standards Board's Contingent Reimbursement Model Code ("the CRM code"). This code requires firms to reimburse customers who have been the victim of authorised push payment ("APP") scams, like the one Mrs H fell victim to, in all but a limited number of circumstances. Only the last four payments Mrs H made were covered by that Code and so I'll discuss those separately.*
>
> *<u>Payments 1 to 11</u>*
>
> *These payments were made by Mrs H to an account in her name with a different business. It was from there that she transferred the funds on to an account controlled by the fraudsters. The CRM Code only offers protection to customers where they've made payment to "another person" – but in respect of these payments, Mrs H paid herself. As a result, the provisions of the Code don't apply.*
>
> *However, as explained above, good industry practice meant that Metro needed to take some steps to protect Mrs H from the risk of fraud. The Investigator concluded that it should've identified the risk when Mrs H made a payment of £11,000 on 7 July. I'm inclined to agree with that conclusion.*
>
> *By that point, Mrs H had moved a significant amount of money in a very short space*

of time and this was the first payment above £10,000. The payments were being made to an account in Mrs H's own name with a third-party firm. That's something that one might reasonably think suggests a lower risk of fraud. However, this was consistent with a pattern of fraud that is well recognised in the industry. I think Metro ought to have been concerned and that the risk that Mrs H was falling victim to a scam was a foreseeable one

However, although I've concluded that there was a clear point at which Metro ought to have intervened, it does not automatically follow that it needs to refund Mrs H. I can't ask it to do so unless I can reasonably conclude that its error was the cause of her loss. I have to take into account the law on this point. That means I need to be able to affirmatively answer the following question – would the damage or loss which Mrs H has complained about have occurred "but for" the failings of the respondent? In other words, is there sufficiently strong evidence to show that it's more likely than not that, "but for" the failing on the part of Metro, the relevant loss would not have occurred? If the loss would have occurred in any event, the actions of Metro were not a "but for" cause.

To reach a conclusion on this point, I need to consider what would have happened if Metro had handled things differently. It ought to have contacted Mrs H and asked her about the payment. It should also have given her general guidance about the prevalence and risk of fraud and scams. However, I'm not persuaded that such an intervention would've made a difference. As I've explained in the background section of this decision, some other banks stopped payments made by Mrs H and called her. She wasn't open and honest with the employees of those banks when explaining what the purpose of the payment was so it's difficult to see how things would've been different if Metro had called her.

The Investigator said that the character of the activity on Mrs H's account was so unusual that, if Metro had intervened, it shouldn't have taken initial answers from Mrs H at face value – essentially, the risk was so much higher that it needed to adopt a more interventionist approach. I'm not persuaded by that argument. Most of the funds that Mrs H lost to the scam were funded by a lump sum payment of around £80,000 that was made into her Metro account. I understand this was from a savings product that had matured. It had presumably been in an interest-bearing product but was now in Mrs H's current account.

I don't think it would've seemed particularly unusual to Metro for those funds to not sit in her current account for a significant length of time. And so, while I agree that it ought to have been concerned enough to call her to discuss the payments, I'm not persuaded that there was such a clear and obvious risk that it ought to have interrogated Mrs H, not accepted her initial answers to its queries or blocked the payments. Overall, I'm not persuaded that any errors on the part of Metro Bank were the cause of Mrs H's losses here and so it doesn't need to refund those payments.

<u>Payments 12 to 15</u>

These four payments weren't made to accounts in Mrs H's name and so they are covered by the CRM Code. The starting presumption under the Code is that the customer should be reimbursed. However, there are circumstances under which Metro wouldn't be obliged to refund her. These are known as exceptions to reimbursement. A firm may choose not to reimburse a customer if it can establish that:

- *The customer 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; or

- *The customer ignored an effective warning in relation to the payment being made.*

There are further exceptions within the CRM code, but they don't apply here

I've considered whether the first exception applies here – in other words, whether Mrs H made these payments without a reasonable basis for believing that the person or business with whom she transacted was legitimate. I accept that Mrs H did sincerely believe that these were necessary steps that she had to take in order to get access to her funds. However, I have to consider whether that belief was a reasonable one or not.

I'm afraid I don't find that it was. I've come to that conclusion for the following reasons:

- *I think she ought to have questioned whether it was realistic that her £500 investment could have yielded a return of nearly £50,000 in just a few months. This ought to have prompted her to check her e-wallet to see if the claim was true.*

- *Mrs H assumed that the individual she spoke to was connected with the business that operated her genuine cryptocurrency account, but the business he claimed to represent had a different name and he doesn't appear to have known about the existence of her account.*

- *It wasn't particularly clear what the purpose was of these later payments that she made to named individuals. She was told that she needed to make them to establish a "link" between her cryptocurrency account and her account with the payment service provider. I don't think this explanation was clear enough that it could justify her being persuaded to transfer such large sums.*

- *Finally, I think she ought to have been concerned at having to pay over £100,000 in order to access a sum of £50,000. While she was given reassurances that many of these overpayments would ultimately be refunded to her, I think she ought to have only proceeded with great caution.*

However, the CRM Code also 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 can be fairly applied (as I am satisfied Metro has established here). Those requirements include the provision of what the Code defines as an "Effective Warning" when a firm identifies an APP scam risk in relation to a payment.

The Code requires that warnings be both specific to the scam risk identified and to be impactful – to positively affect customer decision-making in a manner whereby the likelihood of an APP scam succeeding is reduced. The code goes on to say this should include steps to ensure that the customer can reasonably understand the consequences of continuing with an irrevocable payment.

It's not clear what warning Mrs H would have seen when making these payments. Metro provided us with a list of all of the warnings that she might have seen depending on how

she categorised the payment. However, none of those example warnings directly address the circumstances of the scam that had targeted Mrs H. Even if she had selected 'investment' as the purpose of her payment, she'd have seen a warning that was framed with the intention of protecting a customer from making a new investment. Mrs H believed that she was paying fees to gain access to the proceeds of an investment she'd already made. I don't think the circumstances of this scam were so obscure that it wouldn't be possible for Metro to have tailored the warning more closely to those circumstances.

In summary, I'm not satisfied that the warnings Metro gave were enough to show it complied with the requirements of the CRM Code in relation to these payments. As I have found Metro failed to meet its requirements under the CRM code in relation to payments 12-15, Metro should share liability for the resultant loss with Mrs H and should have reimbursed her 50% of those payments.

Recovery of funds

For completeness, I've also looked into whether Metro did everything it should've done once Mrs H told it she'd fallen victim to a scam.

The first payments were made to an account in Mrs H's name and then transferred on, so it wouldn't have been possible for Metro to recover her funds from that account. However, I can see it did contact the receiving bank in connection with the final four payments promptly (within 90 minutes of the scam being reported). Unfortunately, the funds had already been transferred out of those accounts and so no recovery was possible.

I went on to explain that I was minded to uphold the complaint in part and direct Metro Bank to refund 50% of payments 12 to 15 and to add 8% simple interest per annum to that sum. Mrs H responded to say that she accepted the conclusions of my provisional decision. Metro Bank hasn't responded. Since no further arguments or evidence have been presented, I don't see any reason to depart from the conclusions I set out in my provisional decision. I'm therefore upholding Mrs H's complaint in part.

Final decision

For the reasons I've explained above, I uphold this complaint in part.

If Mrs H accepts my decision, Metro Bank PLC needs to:

- Refund 50% of payments 12 to 15.

- Add 8% simple interest per annum to that sum, calculated to run from the date it declined her claim under the CRM until the date a settlement is paid.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs H to accept or reject my decision before 12 January 2024.

James Kimmitt
Ombudsman