DRN-4784225

The complaint

Mrs E complains that Bank of Scotland plc trading as Halifax did not refund a series of payments she lost to a scam.

What happened

Mrs E received a sum of money and looked for ways to invest it online. She came across a company I'll call 'M' that said it was a green energy investment company that provided start-up capital to green energy companies. Mrs E carried out some checks online and found positive reviews and she saw the company was listed on Companies House. Mrs E signed an agreement with M to take out a three-year loan note for £50,000, in which she was promised returns of over 12% monthly. She made the following transfers from her Halifax account and received the following returns:

Date	Amount	Type of payment
11/03/21	£10,000.00	Faster payment
12/03/21	£25,000.00	Faster payment
13/03/21	£15,000.00	Faster payment
01/04/21	£368.22	Returns into account
30/04/21	£526.03	Returns into account
28/05/21	£543.56	Returns into account
01/07/21	£526.03	Returns into account
05/08/21	£543.56	Returns into account
03/09/21	£526.03	Returns into account

From October 2021 onwards Mrs E did not receive any further returns and it became more and more difficult for her to contact anyone in M. After receiving more excuses as to why they could not pay her monthly instalments, she felt she had been the victim of a scam.

Mrs E raised a scam claim with Halifax who explained they felt this a high-risk investment gone wrong, as opposed to an authorised push payment ("APP") scam. Mrs E disagreed with this and referred the complaint to our service for review.

Our Investigator looked into it and on balance, felt there was enough to conclude Mrs E had been the victim of an APP scam. They therefore assessed the payments under the Lending Standards Board's Contingent Reimbursement Model ("CRM") Code which provides additional protection to victims of APP scams. As they felt Mrs E had a reasonable basis to believe the investment was legitimate when she made the payments, they recommended a full refund of the losses incurred, less any returns received by Mrs E. As well as 8% simple interest from the date of the declined claim to the date of settlement.

Mrs E accepted the view however Halifax disagreed. They did not think there was enough to show M was operating a scam company and they highlighted that at that point the website was running, the company was listed as operating on Companies House and there was no evidence of an investigation against M.

As an informal agreement could not be reached 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.

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 the evidence is incomplete, inconclusive or contradictory, I reach my decision on the balance of probabilities – in other words, on what I consider is most likely to have happened in light of the available evidence and the wider circumstances.

It isn't in dispute that Mrs E authorised the payments in question. Because of this the starting position – in line with the Payment Services Regulations 2017 – is that she's liable for the transactions. But she says that she has been the victim of an authorised push payment (APP) scam.

Halifax has signed up to the voluntary CRM Code, which provides additional protection to scam victims. 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). But the CRM Code only applies if the definition of an APP scam, as set out in it, is met. I have set this definition out below:

...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.

I've considered the first part of the definition, and having done so I'm satisfied that Mrs E paid the account she was intending to send the funds to. And I do not think there was any deception involved when it comes to who she thought she was paying. So, I do not think the first part of the definition set out above affects Mrs E's transactions.

I've gone on to consider if Mrs E's intended purpose for the payments was legitimate, whether the intended purposes she and the company she paid were broadly aligned and, if not, whether this was the result of dishonest deception on the part of the company.

Mrs E believed the purpose was that of an investment providing a fixed rate of return to a green energy investment company which would, in turn, provide small and medium sized renewable energy developers with short term funding. According to the literature it purported to *only ever lend to sophisticated renewable energy investors and experienced renewable energy developers*. However, Mrs E has said she did not have much investing experience at the time, as she had only recently come into some money that she could invest.

Looking at M's records on Companies House – it hasn't posted accounts since 2021 and doesn't appear to have been audited. The nature of the business at the time was listed as development of building projects and, whilst the listing had also included activities auxiliary to financial intermediation by the time Mrs E made her investment, this doesn't appear to be in line with the investment purposes she was led to believe she was investing in. I also note

the business has now dissolved as a result of a compulsory strike-off and they no longer have an online presence in the form of a website.

The FCA (Financial Conduct Authority) provided a warning in October 2021 about M providing financial services when it was not authorised to do so. I can see that Mrs E invested before this date. Z (an organisation that took over M in 2022) told investors the FCA warning was due to clone companies impersonating M - which doesn't appear to be true. And there's no current evidence to suggest a clone company was in operation as Z claimed. While I appreciate this occurred after Mrs E took out the investment, I think it is relevant to the overall picture of M and its legitimacy as a business.

It's also important for me to state that, to date, I've not been provided with any evidence to show that the business was operating in line with the way it described to, and agreed with its investors prior to their investment. So based on the evidence I have, on balance, I don't think the intended purposes of Mrs E and M aligned and I think it's more likely this was due to dishonest deception on the part of M. So, I believe this was a scam.

Are the payments covered under the provisions of the CRM Code?

Halifax has raised concerns that the payments would not be covered under the CRM Code, because they went to an intermediary I'll call 'N', before being passed to M.

However, the CRM Code does not require the initial recipient of a payment to be an account owned by and for the benefit of the fraudster. Neither does it require that account to be controlled by a party which is complicit in the fraud. Instead, the relevant test is whether an APP scam has taken place. As explained above, in this case, I think the payment meets the definition of an APP scam under DS1(2)(a)(ii) in that Mrs E transferred her funds to another person (N) for what she believed was a legitimate purpose but was in fact fraudulent. Specifically, Mrs E believed that she was making a payment as part of a legitimate scheme but, in fact, she was being defrauded.

If the CRM Code required that the first recipient of funds also be the party that benefits from the fraud, a great many claims would be excluded. I say this because many first-generation accounts are not controlled by the fraudster themselves. The use of money mules (complicit or innocent) is well-known and the CRM Code does not require the sending firm to make an assessment of whether the recipient account holder was complicit in the fraud or not.

Instead, I need to consider whether the funds were effectively under the control of the fraudster at the point they arrived at N.

Given what is known of the relationship between N and M it's very likely that they had a pre-existing agreement. More importantly, Mrs E does not seem to have a customer relationship with N, the funds do not appear to credit an account in her name and she had no significant interactions with it. I'm satisfied N was acting on behalf of M and not Mrs E and she had no reasonable way of preventing the onward transfer of funds to M.

It follows then that the money was both out of Mrs E's control at the point it arrived at N and effectively under the control of M. Consequently, the circumstances in this case are not significantly different from a typical scam scenario - where funds are transferred into an account which is unlikely to be owned by the fraudster, but the recipient has agreed to pass funds on to an ultimate beneficiary.

That means that the payments Mrs E made is capable of being covered by the provisions of the CRM Code. The Lending Standards Boards' consultation makes clear that certain multi-

stage frauds are within the scope of the Code.

But, for the reasons I've already outlined, in this case there's no need to consider the payment from N to M (the onward transmission of funds) as the funds were effectively under the control of M once they reached N.

Finally, I've thought about whether it's fair for the CRM Code to apply in such circumstances.

Halifax has suggested Mrs E should contact the liquidator for N (it entered liquidation in August 2021). But, for the reasons I've already set out, the involvement of a genuine (or unwitting) intermediary does not exclude the possibility of the CRM Code applying. Neither do I think it is unfair for the Code to apply.

I am not sure if Halifax accepts it would be liable (at least to consider the complaint under the Code) had the payment been made directly to M. But I think it's fair to say, I think, that the involvement of N was essentially incidental. And, whether the payment went directly to M or to N it's very unlikely it would have found that payment to be unusual and prevented it.

So, while I'm somewhat sympathetic to Halifax that they, rather than another financial business, will be solely responsible for Mrs E's loss, given that Halifax is a signatory to the CRM Code, I don't find that them being responsible creates an unfair outcome. Neither can I direct Mrs E to pursue the matter solely with N which is, in any case, now in liquidation.

Reimbursement under the CRM Code

The starting point in law is that Mrs E is responsible for any payments she's authorised herself. But, as set out, the CRM Code requires a firm to reimburse victims of APP scams that fall under its provisions, unless a firm can demonstrate that one of the exceptions to reimbursement apply. I've therefore considered whether these exceptions apply and have firstly focused on whether Mrs E lacked a reasonable basis for believing that she was dealing with a legitimate investment company providing a legitimate investment.

I've firstly considered the fact Mrs E found M herself by searching online, instead of being cold-called by them. I think this would have added an air of legitimacy to the investment as Mrs E had an active participation in choosing them. The returns promised while high, were not excessive and I don't think they indicated the investment was 'too good to be true'.

The investment material I've reviewed appears professional and there was nothing in the public domain at the time about either M or N that Mrs E could've reasonably inferred from that a scam was taking place. The most persuasive aspect of the scam that I've seen is that M used N, the firm regulated by the FCA at the time of the scam, to gain legitimacy and this was highlighted in the literature.

Did Mrs E ignore an affective warning?

The CRM Code says that effective warnings should be risk based and, where possible, tailored to the APP scam risk indicators and any specific APP scam types identified through the user interface with which the customer is initiating the payment instructions.

I can't see that Halifax provided any warnings or intervened in the payments prior to them being processed. It follows that Mrs E therefore did not ignore an effective warning as Halifax did not provide one for her to take heed of. So, I don't think an exception to reimbursement applied in Mrs E's case.

Recovery of funds

In light of my conclusions above, it is not necessary in this case to consider whether the bank also exercised enough care and urgency in trying to recover the stolen funds from the payee bank before they were irretrievably removed by the scammers. But for completeness, even if there was a delay, I don't think it likely would have made a difference here.
The first three scam payments were made in March 2021 and the scam wasn't reported until November 2022. I understand that Mrs E didn't know she was the victim of a scam before this, but the delay means any recovery action was most unlikely to be successful - as scammers usually remove funds as soon as possible.

Putting things right

Halifax should refund Mrs E the £50,000 she lost to the scam, but should deduct the returns she received into the account from the total. Halifax should also add 8% simple interest from the date of the declined claim to the date of the refund.

If Halifax considers that it's required by HM Revenue & Customs to deduct income tax from that interest, it should tell Mrs E how much it's taken off. It should also give her a tax deduction certificate if she asks for one, so she can reclaim the tax from HM Revenue & Customs if appropriate.

My final decision

I uphold Mrs E's complaint and recommend Bank of Scotland plc trading as Halifax pay the redress outlined above.

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

Rebecca Norris
Ombudsman