DRN-5626611

The complaint

Mrs H complains Bank of Scotland plc trading as Halifax won't refund payments made as part of a scam.

Mrs H is being represented by a claims management company in this complaint.

What happened

The exact details of what happened are unclear. In the complaint letter, Mrs H's representative has explained she was looking for an investment opportunity and after coming across an advert online, she left her information to find out more. She was then contacted by an individual I'll call "O" (who claimed to be from a company I'll call "M"), who said they were offering investment opportunities through cryptocurrency. And in order to invest, she had to send her money to a cryptocurrency account. She says this individual showed her expected returns through remote software and she was told to make more payments to pay tax to then receive her money. But during her conversations with Halifax, when it spoke to her on a few occasions at the time of the payments, Mrs H detailed that O was assisting her in getting her investment returns back as she had previously invested a small sum and had also received returns.

Mrs H's representative further details that the cryptocurrency account was set up after she provided access through a remote software program, but it wasn't her that set up the account, nor did she have access to it. After access was given, it is alleged that O made a payment of £23,000 on 11 July 2023 that Mrs H didn't authorise, though she was unaware of it until the next day when she notified Halifax.

In the call, Mrs H shared the same detail to Halifax about how the account was set-up, and she also described being told to go in and out of accounts and asked to press different buttons. After it asked her to check if she had access to her cryptocurrency account, she said she did and could see a balance that held almost all of the funds transferred the day prior. Halifax referred her back to her cryptocurrency account provider as it said she would need to try and recover her money through the provider.

Mrs H's representative also explains that when she discussed this with O, she was informed that her money was safe in her cryptocurrency account. And as she wasn't aware she didn't have access to her account, she assumed everything was fine.

Mrs H acknowledges making two payments to the same cryptocurrency account on 10 August 2023, one for £900 and another for £2,068. She then contacted Halifax on the same day explaining she had been speaking to someone who was helping her with her cryptocurrency, and she had concerns of possibly being scammed. During the call it was established Mrs H was able to log into her cryptocurrency account and was able to see a balance.

Halifax again referred Mrs H to her cryptocurrency account provider to recover her money. And following that, £2,824.58 credited Mrs H's Halifax account from her cryptocurrency account. There were also further calls on the day where similar discussions happened about

someone contacting her along with her not being sure she could trust them.

Later on in September 2023, a claim was logged and Halifax spoke with Mrs H about her being scammed and the need to stop being in contact with O. This was after it had flagged other scam-related payments where it asked her to get in touch.

Halifax didn't agree to provide a refund, and after Mrs H raised a complaint, Halifax issued its final response letter. In summary it said as the funds had been transferred to her own account, it was limited in what it could do to help. And when Mrs H called about suspected fraud, it referred her back to the cryptocurrency provider and no warnings were provided as it wasn't known at the time if fraud had happened. Unhappy with its response, Mrs H's representative referred her complaint to our Service on her behalf.

One of our investigators looked into Mrs H's complaint but didn't uphold it. They considered Mrs H authorised the £23,000 payment and because of the limited information provided about the scam, they didn't think an intervention could have uncovered a scam. Mrs H didn't agree, with her representative providing a comprehensive response. In summary it said Mrs H hadn't authorised the £23,000 payment and it ought to have stopped and prevented the payments from debiting her account.

As Mrs H didn't agree, the matter was passed to me to decide. I issued a provisional decision where I didn't uphold this complaint. In summary I said I considered Halifax was fair to treat the payment as authorised, and it was likely Mrs H was the victim of a scam. And whilst I thought Halifax ought to have spoken with Mrs H about the payment she made, and this likely would have positively impacted her decision-making, Mrs H hadn't evidenced that the payment she'd made was ultimately lost to the scam. So I concluded that it wouldn't be fair for Halifax to refund her. Halifax didn't have any further comments, and Mrs H's representative didn't agree. I've summarised its points below:

- It said they believe she didn't set-up or have access to the cryptocurrency account. And it was the fraudster that carried out the payment on her behalf and transferred the funds elsewhere.

- It's more likely the reference to seeing a balance was on the scam platform instead of the genuine cryptocurrency platform.

- It believes that the timing of the credit received from the cryptocurrency provider strongly suggests the payments failed and were automatically reversed, instead of them being withdrawn by Mrs H.

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.

Having done so, I still don't uphold this complaint. While I think it was likely Mrs H was scammed and authorised the £23,000 payment, and Halifax's intervention could have positively impacted her decision-making, I'm not persuaded there's evidence that the funds were lost to the scam.

Was Mrs H the victim of a scam?

We can't know for certain exactly what happened, but I consider it important at the first point to set out whether I think it's likely Mrs H was the victim of a scam.

The testimony Mrs H's representative has provided this Service isn't completely aligned to the testimony she provided Halifax when she initially reported and discussed the payments in dispute. There's also a lot that has happened that Mrs H hasn't been able to recall such as her full interaction with O, so it's difficult to establish exactly how things unfolded. I don't think this is because Mrs H is refusing to share this information, but I consider she exhibits vulnerable traits which means that she hasn't been able to provide a clear and consistent overview of what happened. Or recall how things unfolded in detail. And this is evidence from the contemporaneous calls I've been able to listen to.

From what I have been able to establish, Mrs H was dealing with O who claimed to work for M in relation to a cryptocurrency investment. At the time of the £23,000 payment, it appears the conversations Mrs H was having with O was around a previous investment and about getting her money back. She downloaded a remote software program, and a cryptocurrency account was opened in her name that the £23,000 payment – as well as the later two payments she authorised – was then sent to.

Further to that, Mrs H provided this Service a copy of an email she was sent where it detailed a balance she held in excess of £400,000 and mentioned having to pay taxes to release those funds. There's also an online review that comments on this likely being a scam. I consider there are some common hallmarks of investment related scams in Mrs H's circumstances and so I think it's more likely than not she was the victim of a scam, which Halifax hasn't refuted.

Did Mrs H authorise the £23,000 payment?

Halifax considers Mrs H authorised the £23,000 payment, but Mrs H said she didn't. Where Mrs H disputes authorising this payment, I've gone onto consider what I think the more likely scenario is.

In line with the Payment Services Regulations 2017 ("PSRs") – the relevant legislation here – the starting position is Halifax is liable for unauthorised payments, and Mrs H is liable for payments she's authorised.

Mrs H has explained that an account needed to be set up with the cryptocurrency provider but as she was unclear on how to do this and how cryptocurrency worked, O gained access to her device through a remote software program and completed the actions on her device.

The device Mrs H said remote access was given on was her iPhone device. But having researched into the remote access program she said she installed, it confirms that the software is limited in terms of its functionality on devices using the iOS operating system – the manufacturer's operating system. Meaning it would have allowed a third-party to see the information displayed on Mrs H's phone screen, but it wouldn't have allowed them to take control of her device. I've seen no evidence that suggests Mrs H's phone wasn't operating using iOS at the time and so with this in mind, I don't think this is the likely scenario.

Further to that, in the call Mrs H had the day after the £23,000 payment was made, she described being told to go in and out of her account and to "put this in here". Given the method of payment involved – Open Banking – the payment details would have been initiated on the cryptocurrency provider's website or app and Halifax has shown it was then approved from an iPhone device, which is what Mrs H used at the time, and using biometrics. And I haven't seen anything to show that a third-party device was added on the day to have approved this payment. Mrs H also explained she was told to send money from another account into her Halifax account and believed she did for a small amount. However, the only payment I can see that came into Mrs H's Halifax account – the account involved here – on 11 July 2023 was a £23,500 payment that ultimately funded the payment that went

to her cryptocurrency account. So given this, and the limitations of remote software on iPhone devices, I think it's more likely than not that she made this payment, but did so after being coached by O.

Given the conversation Mrs H had with Halifax the next day, it didn't seem she had a full understanding of what happened, or what steps she might have taken, which I think explains why she doesn't recall, or thought she was, making a payment. Mrs H also accepted making the two later payments to her cryptocurrency account, which were carried out in the same way as the £23,000 payment. So I consider this, along with her telling Halifax in calls that she had access to the account and could see a balance, supports that she had access to her cryptocurrency account where she otherwise said she didn't. And that she had access to have made the £23,000 payment.

I've considered the points raised by Mrs H's representative in response to my provisional decision – that it believes Mrs H didn't set-up or have access to the cryptocurrency account, and that it was the fraudster that carried out the payment. But as I've set out above and in my provisional decision, it wouldn't have been possible. And further to that, there is strong evidence Mrs H was accessing the cryptocurrency account, not the scam platform, where it was mentioned in the call, and she confirmed logging into that platform.

Overall, I consider Halifax was fair to treat the £23,000 payment as being authorised. So in line with the PSRs, Mrs H is liable for the loss, along with the two later payments she authorised. But I've gone onto consider whether Halifax ought to have recognised Mrs H was at risk of financial harm and whether an intervention would have made a difference.

Should Halifax have recognised Mrs H was at risk of financial harm and would an intervention have made a difference?

Though the starting position is that Mrs H is liable for this payment, taking longstanding regulatory expectations and requirements into account and what I consider to be good industry practice at the time, Halifax should fairly and reasonably have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances.

Having considered the £23,000 payment, and Mrs H's recent activity prior to it being made, I consider the payment was out of character for her account. Considering the recent activity, it wasn't common for Mrs H to make larger payments from her account. And along with it going to a cryptocurrency provider, it was a significant increase in spending suggesting a heightened risk of fraud. So I consider Halifax ought to have spoken with Mrs H about the payment before processing it.

Had Halifax spoke with Mrs H, I consider it more likely than not that it would have been on notice Mrs H was falling victim to a scam. In the conversation she had with Halifax the following day after the payment was made, she didn't fully understand what had happened or that a payment was going to be made from her account. I think with proportionate questioning from Halifax, Mrs H would have shared that she thought she was speaking to someone about a previous investment she had, and they were helping to get her money. She was being told what she needed to do and what buttons to click, and she had downloaded remote software. And with that information, Halifax would have been able to warn her she was likely falling victim to a scam, and I think it's more likely than not that she would have heeded the warning provided and wouldn't have proceeded further with making this payment, or the later two in August 2023.

What I think further supports this is that when Halifax spoke with Mrs H in September 2023, and provided sufficient warnings about this being a scam, this appears to have been taken in

by Mrs H. And whilst I note Mrs H did speak to Halifax several times shortly after the payments were made in July and August 2023, it has accepted that the conversations were more directed on her referring back to the cryptocurrency provider to try and recover her money, rather than providing warnings.

Would it be fair to hold Halifax liable for Mrs H's loss?

As I've concluded earlier, I consider Mrs H had access to her cryptocurrency account, and when she discussed the £23,000 payment with Halifax the day after it was made, and it asked her to check her account, she confirmed there was a balance held. And she confirmed most of the funds remained. Halifax referred Mrs H back to the cryptocurrency provider to withdraw those funds, but it remains unclear what happened following her call with Halifax.

Mrs H's representative argues that the fraudster transferred the funds elsewhere. But this Service has given Mrs H and her representative multiple opportunities to provide evidence showing the £23,000 amount was later lost to a third-party. Including further opportunities after I issued my provisional decision. But no evidence has been provided. And while I don't dispute Mrs H has exhibited vulnerabilities, I've not been provided with an explanation as to why, with her representative's assistance, this information can't be provided given the evidence supports she had access to her cryptocurrency account and a balance was available the day after the payment was made.

Further to that, we've also asked for evidence around the initial payments she said she made earlier, and other returns she said she received, but this hasn't been forthcoming. I note Mrs H has other accounts with Halifax and she told Halifax she downloaded a banking app for an e-money account provider. This suggests that different accounts may have been used, and so while it's possible the funds were lost to the scam, I also can't rule out the possibility that the funds were returned to a different account.

After making the two payments to her cryptocurrency account in August 2023, Mrs H spoke with Halifax where it referred her to the cryptocurrency provider to seek recovery of the funds. And following that call, the majority of the funds were paid back. So I think it's also possible that the £23,000 could have also been returned as similar conversations were had around this payment. Mrs H's representative said it believes the evidence suggests the payments made in August 2023 failed and were automatically reversed. But I haven't seen any evidence here that supports that's the case. So I don't consider this to be the likely scenario here.

Because of what I've explained above, and the overall circumstances, I can't be certain here that Mrs H's money was later lost to the scam. Whilst I've concluded that Halifax ought to have prevented Mrs H's payments, in order for me to decide that Halifax ought to provide a refund to Mrs H, subject to any considerations around contributory negligence – that I've not considered here due to the lack of evidence of loss of funds to the scam – I need to be satisfied that her money was lost to the scam. I'm in no way disregarding Mrs H has been the victim of a cruel scam however for the above reasons, I don't think it would be fair for Halifax to refund the £23,000 when there's no evidence that it was lost to the scam.

My final decision

My final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs H to accept or reject my decision before 21 July 2025.

Timothy Doe
Ombudsman