

The complaint

Ms M has complained that Bank of Scotland plc (trading as “Halifax”) hasn’t fully refunded the money she lost as part of an investment-related scam.

What happened

The background of this complaint is already known to both parties, so I won’t repeat all of it here. But I’ll summarise the key points and then focus on explaining the reason for my decision.

Ms M has used a professional representative to refer her complaint to this service. For the purposes of my decision, I’ll refer directly to Ms M, but I’d like to reassure Ms M and her representative that I’ve considered everything both parties have said.

Ms M has explained that in November 2020 she decided to start investing in cryptocurrency after it was recommended by a friend, who Ms M says was making good returns on her investment. Ms M spoke to an individual (“the scammer”) at an alleged investment company and she says she was told the capital she invested was guaranteed to be returned to her. She’s also said the scammer sounded professional and knowledgeable, and she did some research on the company and having done so, she decided to invest based on the positive reviews she’d found.

Ms M says the scammer opened an account with a cryptocurrency wallet provider on her behalf and she made six payments to it from her Halifax account. She then converted these payments into cryptocurrency and forwarded them on to what she believed to be her investment account, although she later discovered this was in fact a scammer. She says she was given access to an investment platform which showed her alleged investments and the returns they were making. Ms M also received two payments from the cryptocurrency platform.

The payments Ms M made and received in relation to this scam were as follows:

Date	Amount (£)
19/11/2020	15,000
26/11/2020	5,000
08/12/2020	1001.30 (credit)
11/12/2020	10,000
15/12/2020	1,002.30 (credit)
14/01/2021	10,000
08/03/2021	14,000
29/03/2021	7,000
Total	58,996.40

Ms M realised she’d been scammed when she was unable to make a large withdrawal of the profits she believed she’d made. She also says the scammer demanded more and more

funds in order to cover “fees”, and when Ms M refused to make these additional payments, the scammer stopped contacting her.

Ms M made a complaint to Halifax. Halifax didn’t uphold the complaint as it said Ms M had made the payments to an account in her own name, and she then converted the pounds into cryptocurrency and forwarded it on to the scammer. It also said it intervened before Ms M made three of the payments, and it gave her appropriate warnings about the risks involved with the payments, and Ms M chose to proceed. Ms M remained unhappy so she referred the complaint to this service.

Our investigator considered everything and didn’t think the complaint should be upheld. She explained that although Halifax intervened before Ms M sent a number of the payments, Ms M chose to proceed to make them despite the warnings Halifax gave and the concern it expressed. She also didn’t think that based on Ms M’s reassurances, Halifax should’ve refused to process the payments.

As Ms M didn’t accept the investigator’s opinion, the case has been passed to me to make a 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.

I’m sorry to disappoint Ms M but having considered everything I’m afraid I’m not upholding her complaint, broadly for the same reasons as our investigator, which I’ve set out below.

In broad terms, the starting position is that a firm is expected to process payments and withdrawals that its customer authorises, in accordance with the Payment Services Regulations and the terms and conditions of the customer’s account. And in this case it’s not in question whether Ms M authorised these payments from leaving her account. It’s accepted by all parties that Ms M gave the instructions to Halifax and Halifax made the payments in line with those instructions, and in line with the terms and conditions of Ms M’s account.

But that doesn’t always mean that the business should follow every instruction without asking further questions or intervening to ensure requests coming from their customers are firstly genuine, and secondly won’t result in harm.

There’s no doubt that the payments in question were unusual for Ms M’s account, so Halifax should’ve treated them as such. They were larger than any other payments Ms M had made in the previous six months, and they were being made to an identifiable cryptocurrency platform. So I’ve considered at which point Halifax should’ve intervened, what a proportionate intervention would’ve looked like, and if I think Halifax should’ve done something differently, whether that would’ve led to a different outcome for Ms M.

Halifax says that due to the time that has passed since the payments were made it doesn’t have a record of what warnings, if any, it showed Ms M before the payments were made. But that’s not surprising since they were made almost four years ago.

In its initial complaint to Halifax Ms M’s representative said “Throughout the duration of the scam, you failed to contact your customer in any entirety whatsoever”. But having reviewed everything, I can see that Halifax asked Ms M to contact it by phone on three separate occasions before it released the payments. Halifax has provided recordings of those calls and although I won’t transcribe them fully here, I’ll summarise the salient points.

The first call was made on 19 November 2020 when Ms M attempted to make the first payment, for £15,000. Halifax starts by confirming the purpose of the payment, and Ms M tells it her partner is trading in cryptocurrency and he'd convinced her to join him. Halifax checks whether Ms M's partner had previously had any issues, which she confirmed he hadn't. Halifax told Ms M that the payment showed characteristics of higher risk than normal, and confirms that even if she doesn't receive any goods or services, Halifax might not be able to recover it. Ms M explains that the money is "insured" and Halifax tells Ms M she might've been contacted by a fraudster promising unrealistic returns and gives an example of cryptocurrency investments. It confirms whether Ms M still wants to make the payment, despite what she'd been told, and Ms M confirms she'd like to proceed on the basis that she'd done "a lot of homework" and knew exactly what she was doing. Finally Halifax asks Ms M whether the investment company is FCA registered, which she says it is, and Halifax also checks that the payment is being genuinely made on Ms M's instruction, and she's under no pressure to make it. Ms M confirms this to be true, and the payment is released.

The next call was made before the second payment was made, on 26 November 2020. In this call Ms M confirms this is the second payment to the same payee, and she tells Halifax she's investing in cryptocurrency, to which Halifax lets her know there's a lot of fraud related to cryptocurrency at the time, and Ms M confirms she's fully in control of the funds. Halifax again tells Ms M that the payment appears to show higher than usual risk characteristics, and that it's difficult to recover it if it's fraudulent. There are some further questions from Halifax to establish that Ms M isn't being monitored or pressured, and Ms M volunteers information that the money she's sending is "insured" and being done via an agent, and Halifax explains that it's concerned by what Ms M has said. Halifax asks Ms M why there is an agent involved and she explains it's because he knows when to trade, and she reassures Halifax that she makes profits as a result.

Finally Halifax explains that if this is ultimately a scam, for example because the agent starts to request she pays money in order to make withdrawals, Halifax won't be able to do much for her. Ms M reassures it that everything is in order and she has full trust, and she's "certain that it's OK". Halifax warns Ms M multiple times through this exchange to "be careful", which Ms M reassures it she will, and the payment is released.

In the third call, which took place on 11 December 2020 when Ms M was making the third payment, Halifax asks Ms M if she's made a payment to the recipient before, which she confirms she has. It confirms the receiving account details and reference for the payment, and the amount, and it then releases the payment with no further questions. In this call there was no attempt to understand the reason for the payment or to give any scam-related warnings.

Finally, Halifax spoke to Ms M on 15 December 2020 as she was unable to log in to her online banking service. Halifax explains that the previous payment was still awaiting a fraud check, and this is what had prevented Ms M being able to log in.

Halifax explains that there's a concern the payment is related to a scam and asks Ms M to give some more details about the circumstances. Ms M explains the payment is for cryptocurrency, and that she'd received a payment from the same company on the same day. She confirms to Halifax that her partner was generally managing the cryptocurrency investments. Halifax explains that there are a lot of scams whereby scammers contact customers purporting to be from legitimate investment companies, but Ms M says this is all being done by her partner, whom she trusts. This call isn't related to a payment but the online login issue is rectified and the call ends.

Halifax didn't intervene in the final three payments, and in the circumstances, I think that's reasonable. It had spoken to Ms M previously four times, and it had been satisfied during three of those calls that Ms M was aware of the risks involved with fraud and scams, and that she was fully in control of the payments she was making, and the reasons she was making them.

Given the content of the previous calls I'm persuaded that even if Halifax had intervened every time Ms M made a payment related with this scam, it's unlikely the scam would've been uncovered. I say this because I'm persuaded that Ms M would've been equally insistent that they were related to a legitimate investment. I appreciate this was Ms M's genuine belief at the time, and I think it was reasonable for Halifax to accept Ms M's answers as truthful without unduly interrogating her, so I don't think the scam would've been uncovered no matter how many more times Halifax had intervened.

In balancing its responsibility to protect its customers without unduly inconveniencing them, I don't think it was unreasonable for Halifax to consider the cryptocurrency exchange as a trusted payee after the first three payments. It wouldn't be practical or reasonable to expect a bank to stop every payment that fell outside of usual day-to-day spending, and in this case, I'm satisfied that Halifax had done enough to satisfy itself that Ms M wasn't at risk of harm by paying this payee, without having to repeat its interventions for every subsequent payment.

In considering Halifax's shortcomings it was also fair that I considered the action Ms M took before sending funds to the alleged investment.

Ms M has explained that she was guaranteed a return of 100% of her initial investment, although I'm not aware that she ever received any paperwork or documentation in relation to it.

Although I accept Ms M was an inexperienced investor, I agree with Halifax that it's too good to be true that any capital invested would be 100% guaranteed – and I also don't think inexperience is a valid reason to think that might be true. Ms M also says she was coached on how to answer questions from the bank by the scammer. I think this in itself should've raised suspicion for Ms M, given a legitimate investment company wouldn't need its customer to tell the bank anything other than the truth.

This, plus the fact the opportunity was introduced by a friend as opposed to a regulated adviser, and the lack of documentation in relation to the investments, means this wasn't a realistic investment opportunity. And although I accept Ms M may've been under the spell of the scammer, I think she could and should have done more to prevent the financial harm this situation unfortunately resulted in.

Taking everything into account, I think Halifax acted proportionately in response to Ms M's payments made towards this scam. Whilst it didn't intervene every time, and the third call wasn't effective, I don't think this ultimately changed Ms M's course of action, or led to her investing when she wouldn't otherwise have done so. It's evident from the calls I listened to that Ms M was under the spell of the scammer, and although she acknowledged the various and repeated warnings given by Halifax, she wasn't convinced that these warnings were applicable to her situation, so she chose to make the payments regardless. And for this reason, I'm afraid I don't hold Halifax responsible for what Ms M lost as a result.

I've seen that Ms M's representative believes Ms M should've been referred to one of Halifax's branches to verify the payments, and that it could've successfully intervened under the Banking Protocol.

The Banking Protocol is specifically designed to protect customers from making scam-related payments in-person and encourages banks to work closely with the police in such cases. But as Ms M wasn't in one of Halifax's branches, the Banking Protocol doesn't apply here, and I wouldn't have expected Halifax to send Ms M to a branch when it was able to intervene by phone, as it did here.

Recovery of the funds

Halifax didn't attempt to recover the funds Ms M lost as part of this scam. It wasn't made aware of the scam until over three years after the payments were made, and Ms M had sent the funds to her own account held elsewhere, which she'd then forwarded on to the scammer.

With both of these points in mind, there was no realistic prospect of a successful recovery so I don't think recovery was a realistic route that Halifax should've pursued.

I'm very sorry that Ms M has fallen victim to this scam and I do understand that my decision will be disappointing. But for the reasons I've set out above, I don't hold Halifax responsible for that.

My final decision

I don't uphold Ms M's complaint against Bank of Scotland plc trading as Halifax.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms M to accept or reject my decision before 2 December 2024.

Sam Wade
Ombudsman