DRN-5608328

The complaint

Mr K complains that Bank of Scotland plc, trading as Halifax, won't refund the money he lost to an investment scam. Mr K is represented in this complaint, but I'll refer to him as it's his complaint.

What happened

The detailed background to this complaint is well known to both parties. So, I'll only provide a brief overview of some of the key events here.

In or around August 2024, Mr K was contacted by X (the scammer), on a social networking service, about an investment.

He started to speak to X, who said she was a financial analyst and a business mentor, on a messaging app. X introduced Mr K to a broker called Company Z and Investment Platform P. Mr K could see realistic investment graphs and he thought they were official and legitimate. Also, he could see people making money from bitcoin.

Mr K says he researched cryptocurrency, Company Z and the investment platform and then started to invest. He explains that the P Platform showed him he was making a profit on a daily basis, which gave him further reassurance that the investment was legitimate. Also, each day he would speak to X and Company Z. Mr K started to build a relationship and trust with X, who said she was religious, and he was convinced she was genuine and helping him.

Mr K had accounts with Halifax, Bank H, Bank N and Firm R and he transferred funds from these accounts to his accounts with crypto exchanges and then onto the scammers' crypto account.

The scammers' tactics were:

- To show Mr K that he was making significant profits and that to make higher profits, he needed to pay them fees.
- For X to encourage him to invest and, when he doubted the investment and got frustrated and annoyed, to persuade him that it was legitimate and to pay more and more fees until he had given them all his money. Also, to persuade Mr K, X would explain the fees, withdrawal issues and how successful his investment had become. Also, when he struggled to pay the fees, she agreed to make fake contributions.

Under the spell of the scammers Mr K transferred the following amounts between 13 August 2024 and 24 October 2024:

- £12,500 from Bank R – 13 to 23 August 2024
- £17,804 from Bank H – 16 August 2024 to 24 September 2024
- £18,550 from Bank N – 9 to 11 September 2024
- £36,400 from Halifax – 13 September 2024 to 24 October 2024

The £36,400 from his Halifax account went to his account with crypto exchange Company C and was comprised of the following amounts:

Payment Number	Date	Payment method	Beneficiary	Amount £
1	13/9/24	Faster Payment	Mr K's account with Company C	6,000
2	17/9/24	Faster Payment	Mr K's account with Company C	5,200
3	26/9/24	Faster Payment	Mr K's account with Company C	2,500
4	26/9/24	Faster Payment	Mr K's account with Company C	5,000
5	26/9/24	Faster Payment	Mr K's account with Company C	300
6	30/9/24	Faster Payment	Mr K's account with Company C	5,300
7	30/9/24	Faster Payment	Mr K's account with Company C	100
8	7/10/24	Faster Payment	Mr K's account with Company C	4,800
9	7/10/24	Faster Payment	Mr K's account with Company C	200
10	18/10/24	Faster Payment	Mr K's account with Company C	4,300
11	18/10/24	Faster Payment	Mr K's account with Company C	200
12	24/10/24	Faster Payment	Mr K's account with Company C	2,300
13	24/10/24	Faster Payment	Mr K's account with Company C	200
Total				36,400

Mr K realised he'd been scammed at the point he thought his investment was worth £785,000. He wanted to withdraw £100,000 but couldn't afford fees which had a deadline.

Mr K complained to all four banks.

In his complaint to Halifax he requested a refund of the £36,400 he had lost and 8% interest because their interventions didn't go far enough.

Halifax rejected Mr K's complaint and refund claim. Their response included the following points:

- They would've expected Mr K to have carried out independent checks on the company and the person he was speaking to and checked the Financial Conduct Authority's (FCA) website as well as Companies Houses.
- The returns Mr K was offered were too good to be true and this should've been a cause for concern.
- They did try to protect him:
    - They declined the first payment and spoke to him, but he wasn't honest saying no one was helping him with the investment and he was doing it independently.
    - They told him about the risks involved in investing in crypto, but he advised he still wanted to make the payment.
    - They intervened several times but Mr K was consistently dishonest about what he was doing.

Mr K was dissatisfied with Halifax's response and brought his complaint to our service adding that he *'had no reason to lie or evade questions from the bank'.*

However, upon listening to recordings of interventions from Halifax and Bank H our investigator didn't think Halifax should reasonably have been expected to prevent the scam.

As Mr K remains dissatisfied his complaint has been referred to me to look at.

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, whilst I'm very sorry to hear that Mr K has been the victim of this cruel investment scam and lost a significant amount of money here, I'm not upholding this complaint. I'll explain why.

I should first say that:

- Although I don't underestimate the severe impact this has had on Mr K, I must approach this matter objectively.
- I've carefully considered all the points Mr K and Halifax have made and I've focused on what I think are the important points to reach a final decision.
- I'm satisfied that the Contingent Reimbursement Model (CRM) and then the APP Scam Reimbursement Rules, introduced by the Payment Systems Regulator in October 2024, for customers who have fallen victim to an APP scam, don't apply here as the payments Mr K authorised were to another account under his control.
- The Payment Services Regulations 2017 (PSR) and FCA's Consumer Duty are relevant here.

  <u>PSR</u>

  Under the PSR and in accordance with general banking terms and conditions, banks should execute an authorised payment instruction without undue delay. The starting position is that liability for an authorised payment rests with the payer, even where they are duped into making that payment. There's no dispute that Mr K made the payments here, so they are considered authorised.

  However, in accordance with the law, regulations and good industry practice, a bank should be on the look-out for and protect its customers against the risk of fraud and scams so far as is reasonably possible. If it fails to act on information which ought reasonably to alert a prudent banker to potential fraud or financial crime, it might be liable for losses incurred by its customer as a result.

  Banks do have to strike a balance between the extent to which they intervene in payments to try and prevent fraud and/or financial harm, against the risk of unnecessarily inconveniencing or delaying legitimate transactions. So, I consider Halifax should fairly and reasonably:

  - Have been monitoring accounts and any payments made or received to counter various risks such as anti-money laundering and preventing fraud and scams.
  - Have systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which banks are generally more familiar with than the average customer.
  - In some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, before processing a payment, or in

some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

Consumer Duty

Also, from July 2023 Halifax had to comply with the Financial Conduct Authority's Consumer Duty which required financial services firms to act to deliver good outcomes for their customers. Whilst the Consumer Duty does not mean that customers will always be protected from bad outcomes, Halifax was required to act to avoid foreseeable harm by, for example, operating adequate systems to detect and prevent fraud.

With the above PSR and Consumer Duty in mind, I considered whether:

Halifax identified that Mr K was at risk of financial harm and put in place proportionate interventions?

Halifax have provided information which shows Mr K's payments triggered automated warnings which included being signposted to their fraud hub. However, these warnings weren't relevant due to Mr K having selected that the payments were going to friends and family.

However, although Mr K did make large payments from his account and his above-mentioned friends and family selection suggests he was looking to avoid an intervention, I found that, upon his first payment to the crypto exchange, Halifax did recognise this payment was unusual and high risk.

So, at payment number 1, for £6,000, they put in place an intervention call with one of their fraud and scam agents, who asked Mr K what he intended to do with funds after they left his Company C account and establish if he had a broker or financial advisor.

Although Halifax approved payment 1, payment 2 for £5,200 was only a few days later and they stopped this several times and put in place a second human intervention, which again discussed the risks and probed what Mr K was doing in order to protect him from financial harm.

Halifax have explained that after strong interventions on the first two payments, which equated to nearly a third of the payments to Company C, the spend on the account was normalised with no further human intervention. Considering all of the subsequent payments were for lower amounts than payment number 1 and spread over an approximate six-week period, if the interventions were effective, I think these would've been proportionate.

After establishing that Halifax did recognise a risk and put in place interventions I then considered:

The effectiveness of Halifax's interventions and why they, together with an intervention from Bank H, didn't prevent Mr K's loss?

I found that Halifax put in both an automated and human intervention on payment number 1.

Regarding the automated intervention the information was largely irrelevant as Mr K selected friends and family as the reason. However, Mr K was signposted to scam information on Halifax's fraud hub and because of the heightened risk (a large payment for £6,000 to a crypto exchange) Halifax stopped the payment and put in place an intervention call with one of their fraud and scam agents. I consider this action to have been proportionate.

Also, I noted that when:

- Bank H gave Mr K several automated warnings he incorrectly said he was paying a bill and family / friends. Nonetheless, he received some relevant warnings and still decided to proceed.
- Bank N put in a strong tailored automated intervention about crypto payments and

bitcoin that were directly relevant to the scam Mr K still chose to proceed.

Halifax implemented three intervention calls on 12,13 and 17 September 2024 (week 5 and 6 of the 11-week scam period), prior to releasing payment 1 and 2.

I listened carefully to these calls. Also, to an earlier intervention call which Bank H put in place at week 2 of the 11-week scam period.

Although there isn't any evidence that coaching took place to reduce payments and counteract interventions and Mr K says he *'had no reason to lie or evade questions from the bank'*, I considered this to be a possibility:

- Due to Mr K's selection choices when Halifax and Bank H put automated interventions in place.
- Because I found Mr K wasn't truthful to Halifax when he spoke to their fraud and scam agents. Also, the agent of Bank H.
- Mr K was having daily conversations with the scammers.
- I noted that in his dialogue with X, Mr K discussed the banks he was using and after the Halifax intervention call on 13 September 2024 he said to X:
    - '*What a nightmare. I feel like a criminal all the questions!'*

So, although I don't know if the scammers were coaching Mr K, when listening to Halifax's call recording and Bank H's, I considered whether the agents were alive to the risk of coaching.

An intervention shouldn't be an interrogation; it should be suitable questions designed to unearth a potential scam and establish if the customer is at risk of financial harm.

Although I found some of Halifax's calls to be stronger than others and think the Bank H call could've included more open questions, I found the education and warnings to have been consistently strong.

Mr K was informed:

- Scammers approach people on social media, and the scams include fake brokers, fake platforms and trading accounts.
- Scammers show realistic graphics illustrating profits together with group chats or messages from people making profits.
- The profits will be too good to be true. Scammers pressurise victims to pay more and more money in extortionate fees to access high profits.
- Even when victims can't access fake profits, and they think it may be a scam, they often struggle to accept the reality and continue to pay more.
- Scammers tell and coach victims to move funds between accounts and to lie to their banks.
- Banks continue to see a rise of investment scams with crypto and bitcoin being higher than normal risk. These are volatile due to lack of regulation and therefore due diligence and checking with the FCA is important.

Overall, I found that the probing was strong and when Mr K was asked more open and probing questions by Halifax agents he still gave false and misleading answers. For example, when asked the following questions:

- Why was he investing in bitcoin? How was he introduced to it?
    - He consistently said it was a long-standing male friend who was making money from bitcoin through a crypto exchange company. And when probed

further about his friend, how he knew him and how he communicated with him, he gave false answers.

- Was any third party advising or helping him? Did he have an investment company and broker acting on his behalf? Is he paying exorbitant fees? What research had he done?
    - He consistently said no, which also wasn't the case.
    - Also, he'd done his own research following his friend's advice.
- How does he communicate with a third party or investment company? How does he know the investment company? How does he make withdrawals? Is someone saying you can make loads of money? Who is advising you?
    - He again consistently said it was just him acting on his friend's recommendation.

Also, he was repeatedly told that for the bank to protect him they needed him to be honest and asked if anyone was telling him to lie or manipulating him. And that only a scammer would do so. However, he consistently said no to these questions.

Mr K was asked a number of other questions including why he was transferring funds between his accounts and whether he was gaining high returns in a short space of time.

Most, and perhaps all, of the above scam warnings applied to Mr K. He had been approached by social media, he thought he had a broker, he was surprised the profits were so large (commenting to X that '*When it's too good to be true it usually is*'), he was getting annoyed and frustrated with the extortionate fees and being asked to make more and more payments. At a number of stages, he thought he was being scammed but due to the spell X had over him and the amount of money he had invested had he ignored his own misgivings. Also, others appear to have told Mr K they had misgivings over the investment as he tells X *'Lots of people have told me that this company are scammers'.*

Yet when repeatedly asked questions about whether any of the above applied to what he was doing he said it didn't, and he consistently gave false answers saying he was acting alone after a well-known male friend had given him advice. Regarding the warnings about the high risk of losing all his money, Mr K again accepted the risks.

Regarding Mr K's above comments about how he felt about the Bank B call, which lasted thirty minutes and was a very strong call in terms of education, warnings and probing. I think the Bank B agent may have been suspicious that Mr K was being coached as he repeatedly asked him if anyone was asking him to lie and told him about the importance of giving honest answers to his questions. However, on all the calls Mr K was insistent that no one was telling him to lie, maintains this in his complaint, and it isn't illegal for customers to trade in crypto.

Having considered all the above, even if Halifax put in place further interventions (which I don't think would've been proportionate), I think Mr K would've prevented them from uncovering or stopping the scam.

Finally, with regards to recovery, Mr K's funds were paid into a crypto wallet and then sent on to the scammer, so unfortunately there was no realistic opportunity for Halifax to recover the funds.

I realise the outcome of this complaint will come as a great disappointment to Mr K and I'm very sorry he has lost a significant amount of money here. But, for the reasons I've explained, I won't be upholding this complaint and asking Halifax to make any refund.

My final decision

For the reasons mentioned above, my final decision is that I'm not upholding this complaint against Bank of Scotland plc trading as Halifax.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr K to accept or reject my decision before 20 October 2025.

Paul Douglas
Ombudsman