

## The complaint

Ms F complains that Bank of Scotland plc trading as Halifax (“Halifax”) won’t refund the full amount of money she lost after she fell victim to an ‘authorised push payment’ (“APP”) scam.

## What happened

The background to this complaint is well-known to both parties, so I won’t repeat it in detail here. But in summary and based on the submissions of both parties, I understand it to be as follows.

Ms F complains that from September 2022 she made three payments to what she thought was a legitimate cryptocurrency trading company from her Halifax account.

20/09/2022	£20,000	Faster payment
29/09/2022	£25,000	Faster payment
04/10/2022	£3,000	Faster payment
Total	£48,000	

Ms F says she spotted an advertisement on a social media platform advertising a cryptocurrency investment opportunity. Ms F completed an online enquiry form, and she was then contacted by someone from the company.

After completing some Identification checks, Ms F sent three payments to the scammer with the understanding that she was investing in cryptocurrency. When Ms F couldn’t withdraw any money from the cryptocurrency account, she realised she had been scammed and logged a claim with Halifax.

Halifax didn’t think it had done anything wrong by allowing the payments to go through, as it said it called Ms F on each of the payments to warn her of potential scams and she still wanted to make the payments. So, Ms F brought her complaint to our service.

Our investigator looked into the complaint but didn’t think it should be upheld. Our investigator found Halifax had taken steps to warn Ms F of the potential scam, but Ms F ignored the warnings.

Ms F didn’t agree with the investigator’s view, so the complaint’s 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.

Having done so, I’ve come to the same outcome as the investigator for largely the same reasons. I’ll explain why.

I'm very aware that I've summarised this complaint briefly, in less detail than has been provided, and in my own words. No discourtesy is intended by this. Instead, I've focussed on what I think is the heart of the matter here. If there's something I've not mentioned, it isn't because I've ignored it. I haven't. I'm satisfied I don't need to comment on every individual point or argument to be able to reach what I think is the right outcome. Our rules allow me to do this. This simply reflects the informal nature of our service as a free alternative to the courts.

### Prevention

In broad terms, the starting position in law is that a bank is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. And I have taken that into account when deciding what is fair and reasonable in this case.

I'm satisfied that although Ms F didn't intend for her money to go to a fraudster, she did authorise the payments. I understand she wouldn't have authorised the payments if she had known this was a scam, but Halifax is expected to process payments that a customer authorises or instructs it to make, and that is what it did. The Payment Services Regulations (PSRs), state that payments are authorised if the payer consented to them and, in this case, I'm satisfied Ms F consented to the payments as at the time, she believed she was making payments for the purposes of a legitimate investment.

However, where the customer has been the victim of a scam, it may sometimes be fair and reasonable for the bank to reimburse them even though they authorised the payments.

Taking into account the law, regulatory rules and guidance, relevant codes of practice and what I consider having been good industry practice at the time, I consider Lloyds should fairly and reasonably:

- Have been monitoring accounts – and any payments made or received – to counter various risks, including anti-money laundering, countering the financing of terrorism, and preventing fraud and scams;
- Have had systems in place to look out for unusual transactions or other signs that might indicate its customers were at risk of fraud (amongst 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; and
- 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.

Our service has referenced the relevant rules, codes of practice and good industry practice at the time in many previous decisions published on our website.

It's clear the payments looked unusual for the previous spending on Ms F's account, as Halifax flagged them for additional checks.

Having seen the transcripts and listened to the calls Ms F had with the advisors from Halifax, I'm satisfied the advisors asked an adequate amount of questions to attempt to unearth any financial harm Ms F was subjected to and there was no reason to ask Ms F to visit a branch for further checks. I'm also satisfied with the type of questions asked.

On the two calls, as well as some general questions about the payments, the Halifax advisor

- Advised that they had seen similar payments in other circumstances that turned out to be scams.
- Told Ms F that one of the most common scams is around investments and crypto currency.
- Asked Ms F if she was being aided by another individual to make the payments.
- Asked Ms F if she'd been asked to lie.
- Advised Ms F to go away for 24 hours and complete more research whilst making sure she wanted to make the payments.

Ms F then called back and said she was happy for the payments to be sent; Ms F also said she'd been considering moving the money for three months and had done all the necessary checks, including checking the company was registered.

On both calls, Ms F also said that her best friend had been successful with crypto investments and that she felt moving her money into this type of investment would get a better return for her.

Having considered the above, I'm satisfied Halifax asked enough questions and highlighted the risks to Ms F before processing the payment. Even after blocking the payment for 24 hours, Ms F still wanted to proceed. I don't feel Halifax could've reasonably done anything more here to prevent Ms F from sending the money to the scammer.

It's worth noting that Ms F also mentioned leaving money in her wallet instead of sending it on to invest, to get better returns from the interest it gave. This was something she told the advisor and had she done this, the money wouldn't have been sent on to the scammer. So, I'm not convinced Halifax could have done anything more to prevent these payments.

### Recovery

I've also looked at whether Halifax took the steps it should have once Ms F contacted them to dispute the payments.

After the payments were made, I couldn't reasonably expect Halifax to have done anything further until Ms F told Halifax that she had been scammed.

As the money was sent to a wallet in Ms F's name and then sent to the scammer before Ms F reported it, Halifax wouldn't have been able recover any of the funds.

I realise this means Ms F is out of pocket. I'm really sorry she's lost this money. However, for the reasons I've explained, I don't think I can reasonably uphold this complaint.

### **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 Ms F to accept or reject my decision before 17 October 2023.

Tom Wagstaff  
**Ombudsman**