DRN-5907736

The complaint

Mr M and Mrs M complain that Bank of Scotland Plc failed to protect Mr M from losing money in a scam.

A professional representative, W, has brought the complaint to the Financial Ombudsman Service on the couple's behalf.

What happened

The background to this complaint is well known to both parties, so I won't repeat everything here. In brief summary, W explained that Mr M fell victim to an investment scam which involved several bank transfers being made to a cryptocurrency exchange. From here, these funds were ultimately lost after Mr M purchased cryptocurrency and made transfers to a wallet under the scammer's control.

The disputed payments outlined below were made from Mr M and Mrs M's savings account to the cryptocurrency exchange:

Payment number	Date of payment	Amount
1	19 August 2024	£50
2	20 August 2024	£50
3	18 September 2024	£5000
4	12 October 2024	£10
5	19 October 2024	£50
6	21 October 2024	£5000
7	21 October 2024	£5000
8	22 October 2024	£5000
9	28 October 2024	£5000
10	28 October 2024	£2000
11	29 October 2024	£4500
12	01 November 2024	£5000
13	01 November 2024	£5000
14	01 November 2024	£2000
Total		**£43660**

W argued that Bank of Scotland should reimburse the losses from the scam because it processed the payments without question when they were out of character. Bank of Scotland denied any liability and said it hadn't made any errors.

An investigator here reviewed the complaint and partially upheld it. He recommended Bank of Scotland reimburse 50% of the losses from the third payment onward (minus £5 deduction in light of a credit received into the account), along with 8% compensatory interest. In his view, the bank should have intervened at that point by questioning Mr M, which likely would

have uncovered the scam. However, the 50% reimbursement was fair to account for Mr M's own actions during the scam.

Mr M and Mrs M accepted the investigator's recommendations, but Bank of Scotland did not. Instead, it offered to reimburse 50% of the losses starting from the eighth payment, along with 8% compensatory interest.

Mr M and Mrs M declined this offer, and the investigator maintained his original position. With no resolution reached, the case was referred for a final decision.

In summary, Bank of Scotland's key arguments are as follows:

- In the 12 months preceding the scam, Mr M made two high-value payments from his current account that were comparable to the £5000 savings account transaction identified by the investigator as the point for intervention. The bank argued this meant the payment was not unusual.
- Mr M also had a history within the same period of making multiple payments in a single day, similar to those made on 21 October (the sixth and seventh payment).
- The third payment could reasonably have been viewed as a single, higher-value transaction to a legitimate and reputable cryptocurrency platform. Such activity is lawful and increasingly common.
- The bank said that a payment to a cryptocurrency exchange should not, by itself, be regarded as suspicious or indicative of scam risk.

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 agree with the recommendations of the investigator and broadly for the same reasons. I will set out my key findings below.

Initial Considerations

There's no dispute that these payments were authorised. In broad terms, the starting position at law is that a bank is expected to process payments that a customer authorises it to make, in accordance with the terms and conditions of the account.

Under The Payment Services Regulations 2017 (PSRs), which are the relevant regulations in this case, Mr M would be liable for any payment that he authorised Bank of Scotland to make. The PSRs also do not offer specific protections from losses arising from an authorised transaction.

In addition, the disputed transactions in this case are not covered by The Contingent Reimbursement Model (CRM) Code or the Faster Payment Scheme (FPS) Reimbursement Rules. This is because the payments were directed to Mr M's cryptocurrency account at a crypto exchange.

However, taking into account the law, regulatory rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider that Bank of Scotland should fairly and reasonably:

- Have been monitoring accounts – and any payments made or received – to counter various risks including the prevention of 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.

When should Bank of Scotland have intervened?

Bank of Scotland appears to accept that an intervention should have occurred. The question I must determine is when it ought reasonably to have taken place.

After reviewing the evidence, the investigator's assessment, and the bank's response, I conclude that intervention should have occurred at the third payment, for the following reasons:

- Prior to the third payment, transactions on the savings account over the preceding year were generally under £1000 and involved transfers to and from Mr M's other accounts. The £5000 sent to a cryptocurrency exchange on 18 September was therefore a significantly larger sum.
- Although there had been earlier payments to the cryptocurrency exchange since August 2024, these were minimal and did not exceed £50.
- While not every payment to a cryptocurrency platform requires intervention, Bank of Scotland ought to have appreciated at the time of this payment that a transaction like this carried a higher risk of being linked to fraud or a scam.

  Bank of Scotland has accepted that it could identify the payment as being directed to a cryptocurrency exchange at the time. In view of this, and given the size of the third payment compared with previous account activity, the transaction was sufficiently unusual and concerning to warrant the bank's attention.
- I do not consider the two payments cited by Bank of Scotland in response to the investigator to be materially relevant. They were made from a different account, involved amounts roughly half the size, and were not directed to cryptocurrency exchanges. The same reasoning applies to the bank's argument regarding Mr M having previously made multiple payments on the same day.

While Bank of Scotland did not state this explicitly in its response to the investigator, its offer suggests it accepts that the losses could have been prevented had it intervened. For clarity, I also consider that the scam would most likely have been uncovered at the point of intervention.

Given the nature and size of the payments, I would have expected Bank of Scotland to seek further details about the purpose of the transaction. Although the payment was to a legitimate cryptocurrency exchange, the bank should have probed for specifics during such an intervention. By 2024, Bank of Scotland had, or ought to have had, a good understanding of how cryptocurrency-related scams operate, with victims often transferring funds to an exchange before moving them to a scammer. Appropriate questioning would have addressed this risk.

Had intervention occurred at the third payment, I consider it likely that Mr M would have disclosed details of the investment he believed he was making. This would have revealed that he had been asked by the scammers to download remote access software, and that he

was purchasing cryptocurrency under instruction and then transferring it to a wallet provided by the scammer—clear red flags. If asked how he learned of the investment, his reference to unsolicited WhatsApp messages would have further heightened concern.

I have seen nothing to suggest that Mr M would have ignored warnings or advice from Bank of Scotland about these red flags had they been highlighted to him, or that he would have been prepared to accept coaching from the scammer in the face of such direct flags the bank ought to have been able to impactfully warn him about.

Contributory negligence

It is fair and reasonable to consider whether Mr M bears some responsibility for the loss. While I acknowledge that he was the victim of a scam, there were missed opportunities to recognise warning signs during his correspondence with the scammer. The initial contact via WhatsApp, beginning with an unsolicited message, was highly uncharacteristic of a legitimate investment opportunity. Furthermore, the various explanations provided to persuade Mr M to part with additional funds should have raised significant concerns.

For these reasons, I do not consider it fair for Bank of Scotland to bear full liability for the losses from the point at which I have concluded it should have intervened, and I agree with the investigator that a 50% reduction on this basis is appropriate.

Recovery

Once the scam was reported to Bank of Scotland, there was nothing it could reasonably do in terms of recovering any lost funds. All the funds transferred to the cryptocurrency exchange had already been used to purchase cryptocurrency and were directed to a wallet controlled by the scammer.

Credit from the cryptocurrency exchange

Finally, Mr M and Mrs M did not challenge the £5 deduction recommended by the investigator in light of the credit of that amount from the cryptocurrency exchange on 19 October 2025. I don't think this is unreasonable and therefore I will maintain this in my own direction outlined below.

Putting things right

Bank of Scotland must:

- Reimburse Mr M and Mrs M 50% of the losses incurred from the third to the fourteenth payment, as outlined in the table above;
- Deduct £5 from this total to reflect the credit received from Gemini on 19 October; and
- Pay simple interest on the resulting amount at a rate of 8% per year, calculated from the date of each payment to the date of settlement.*

*If Bank of Scotland considers that it's required by HM Revenue & Customs to deduct income tax from that interest, it should tell Mr M and Mrs M how much it has taken off. It should also give Mr M and Mrs M a tax deduction certificate if they ask for one.

My final decision

My final decision is that I uphold Mr M and Mrs M's complaint in part. Bank of Scotland Plc must put things right as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr M and Mrs M to accept or reject my decision before 5 January 2026.

James Abbott
Ombudsman