DRN-3870711

The complaint

Mr T complains that Bank of Scotland plc trading as Halifax won't refund money he lost to a scam.

Mr T is being represented by solicitors in his complaint.

What happened

The detailed background to this complaint is well known to both parties, so I won't repeat it again here. Instead, I'll focus on giving my reasons for my decision.

The complaint concerns 11 payments totalling £11,434.05 which Mr T made to a cryptocurrency platform from his Halifax account in May and June 2022. He made the payments in connection to a commission-based income opportunity which required him to pay in his own money (in cryptocurrency). But the opportunity turned out to be a scam, with the scammer using the details of a genuine affiliate marketing company.

One of the payments, for £74, came straight back into Mr T's bank account. So, the total loss is £11,360.05.

Sequence	Date	Type	Payee	Amount
Payment 1	31 May	Faster payment	Skrill Ltd	£2.00
Payment 2	1 June	Faster payment	Skrill Ltd	£74.00
	1 June	Credit	Skrill Ltd	£74.00 *(credit)*
Payment 3	1 June	Faster payment	Skrill Ltd	£50.00
Payment 4	1 June	Faster payment	Skrill Ltd	£300.00
Payment 5	1 June	Faster payment	Skrill Ltd	£400.00
Payment 6	1 June	Faster payment	Skrill Ltd	£400.00
Payment 7	1 June	Faster payment	Skrill Ltd	£105.00
Payment 8	1 June	Faster payment	Skrill Ltd	£1,123.05 *(initially blocked)*
Payment 9	2 June	Faster payment	Skrill Ltd	£2,000.00
Payment 10	3 June	Faster payment	Skrill Ltd	£3,000.00 *(initially blocked)*
Payment 11	4 June	Faster payment	Skrill Ltd	£3,980.00 *(initially blocked)*
			Total loss	**£11,360.05**

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 conclusions reached by the investigator for these reasons:

- The starting position is that liability for an authorised payment rests with the payer, even when they are duped into making that payment. There's no dispute that Mr T made the payments using his security credentials, and so they are authorised. But 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.

- I've looked at the operation of Mr T's account. I don't consider the first five payments were particularly unusual or suspicious such that I think Halifax ought to have been concerned. They were in keeping with Mr T's usual account activity. Looking at the statements, it wasn't unusual for him to make payments to the same merchant or payee more than once in the same day. But by the point he authorised payment 6 (see above table), Mr T had already sent four payments to the cryptocurrency exchange. In my view, this pattern of successive payments in a short space of time had become unusual enough to warrant an intervention by the bank. We know Halifax didn't intervene at that point. It did, however, intervene two payments later (payment 8) which Mr T also authorised on the same day. So, I've carefully considered the intervention at that point to gain insight into what is likely to have happened had the bank intervened at the earlier payment.

- Halifax has provided a transcript of the call between the bank and Mr T at the time of payment 8, which the investigator has also shared with Mr T's representatives. I can see the agent informed Mr T that there were a lot of scams involving cryptocurrency prevalent at the time and his payment had flagged for additional checks. They made enquiries about why he had been making all the smaller payments, whether he'd set up the crypto wallet himself, and whether he could see the previous payments credit his wallet. The agent also described the most common scenario of cryptocurrency scams where people are contacted by a third-party regarding money-making opportunities and asked to set up, or assisted in setting up, crypto wallets. Mr T was asked if anyone had been in touch with him telling him to do that or if they had made promises of him making good returns on his funds – he said no.

- Having carefully considered Halifax's questions and Mr T's responses to them, I'm satisfied that the bank's intervention was proportionate in the circumstances involved. Given his answers, Halifax didn't have a reason to be concerned. Afterall, the questions that followed its initial enquiries were based on Mr T's response. I acknowledge that Mr T did mention the name of the company involved in passing. But even if Halifax had asked probed him further, I'm not convinced he would have been forthcoming about what he was doing. He'd already misled the bank by saying no one had promised him returns or asked him to send money. So, I'm not persuaded that further questioning would have led to a different outcome here.

- Mr T's representative has argued that he was put under immense pressure by the scammer and that Halifax should be aware that consumers are coached by scammers and may therefore be dishonest. The representative submits that multiple effective interventions and provision of scam warnings could have helped break the spell Mr T was under. I've carefully considered these comments, but I'm not persuaded by them. As I've explained above, I'm not convinced that Mr T would have been forthcoming with his answers had Halifax questioned him further at the time or again at a later point – which it did on two further occasions. While the bank didn't provide an explicit scam warning at those times, it did ask Mr T what the payment was for. This gave him further opportunity to explain what he was doing. But Mr T didn't offer anything more than what he'd previously said. If, as his representative appears to have acknowledged, Mr T was coached into lying, I'm not persuaded

further questioning by Halifax would have led to the scam being uncovered in the way that has been suggested.

- I've also thought about Halifax's actions in relation to the recovery of payments after it became aware of the situation. It isn't clear whether Halifax contacted the beneficiary payment service provider to request a recall of the funds. But the beneficiary account in this case was Mr T's crypto wallet. As he's told us he'd already transferred out the cryptocurrency to the scammer's crypto wallet (albeit he didn't know that at the time), by the time he notified Halifax about the scam there would have been nothing left to recover if Halifax had contacted the payment service provider servicing Mr T's crypto wallet. In the circumstances, I don't think Halifax acted unfairly or unreasonably.

In summary, I know that Mr T will be disappointed with this outcome. Not least because he's told us about the impact this has had on his personal circumstances and the matter has been ongoing for some time. I fully acknowledge that there's a lot of money involved here. Despite my natural sympathy for the situation in which he finds himself, for the reasons given, it wouldn't be fair of me to hold Halifax responsible for his loss.

My final decision

For the reasons given, my final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr T to accept or reject my decision before 19 November 2023.

Gagandeep Singh
Ombudsman