DRN-5651167

The complaint

Ms G complains that Bank of Scotland plc trading as Halifax didn't do enough to protect her from the financial harm caused by a task-related cryptocurrency scam.

Ms G has been represented by a claims management company throughout her complaint. I have referred to them as Ms G's representatives.

What happened

Ms G was approached about doing part time work remotely. She enquired further and not long after, she received a message in WhatsApp, from someone to discuss the job with her. He gave her details about the job, including how she could earn commission from reviewing products.

Ms G was unfortunately in discussions with a scammer, and she was being persuaded to send over money in a sophisticated task-related cryptocurrency scam. The discussions between the scammer and Ms G, and the scam itself lasted for around 4 months, between June and October 2023, with the scammer first making contact on 11 June 2023.

The premise of the scam was that whenever Ms G completed a set of tasks in order to obtain commission, she would instead create a negative balance on her account, and in order to receive her earnings, she would first need to clear the balance by making a payment. The scammer on each occasion would reassure her that this was normal and that she was in fact lucky, as she received combination tasks that attracted more money. He would then inform her that she would receive her money back with commission, if she made a payment to clear her balance. But this was never forthcoming, and another larger negative balance would appear for Ms G to clear. This scam continued throughout the 3 months, with Ms G slowly getting into further problems, with larger amounts to repay.

To begin with in June 2023, Ms G attempted to withdraw a large sum of money with a third-party bank. This triggered an intervention and subsequent warning. With the response it received from Ms G, the third-party bank decided to restrict her account for a period of time.

From 21 July 2023, Ms G decided to switch her efforts in getting her money to the scammers, to another bank. So, she transferred money from her Halifax account to a cryptocurrency exchange account also in her name. In total, she made 27 transfers, with regularity up to 9 October 2023. Ms G through her representatives, made a complaint to Halifax and said she had been scammed for a total of £42,325. Ms G's representatives said Ms G's losses would have been significantly reduced if Halifax had stopped her from making the payments.

Halifax said in response, that it didn't think it needed to intervene, as the payments were not unusual. It said Ms G made the payments through open banking and so there was no requirement for an intervention. It said, even if it did, at any stage, it felt Ms G would have gone ahead and made the payments to the scammer anyway.

Ms G's representatives were not in agreement with Halifax and so referred her complaint to our service.

An investigator from our service said she didn't think Halifax needed to take any further action. She was persuaded Halifax ought to have intervened from the 15th payment made to the cryptocurrency provider, but didn't think it would have made a difference anyway. She concluded Ms G was determined to make the payments, and there was evidence provided that showed an intervention of any kind from Halifax wouldn't have made a difference.

Ms G's representatives didn't accept the investigator's findings. It said Halifax failed to identify a large number of high-risk transactions and it should have contacted Ms G directly. It said Ms G felt the WhatsApp messages had been mis-represented and mis-applied.

The investigator, then contacted the third-party bank that had made an intervention earlier in the scam. She was able to listen to what had been discussed between it and Ms G. She could hear that it had warned her specifically about cryptocurrency scams and details about what she was involved in, including that the person she was trying to make a payment to was a scammer, and had a fake website. The investigator concluded that even though she was told this, Ms G wanted to proceed with the transfer regardless but couldn't with the third-party bank because it restricted her account.

Ms G's representatives made the following points in response and said it would like a review from an ombudsman. It said:

- Halifax should have identified and warned Ms G about the risks involved in making the payments.
- The third-party bank blocked the payments and restricted Ms G's account; however, Halifax took no such action.
- Halifax failed to identify the payments were made to obtain cryptocurrency, with the risks being higher.
- Ms G felt Halifax breached its fiduciary care to her in protecting her from this scam.
- Halifax ought to have acted in a similar way to the third-party bank, by identifying risks were high, raising risk of the scam with Ms G and then blocking the payments.

The parties are still not in agreement, so Ms G's complaint has been referred to me for 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.

Halifax are signed up to the Contingent Reimbursement Model (CRM) that was designed to deal with authorised push payment scams. That said, the code doesn't cover payments that are made by someone, to another account in their name. So, I don't think the code applies here and I've therefore not considered this any further.

Under The Payment Services Regulations and the terms and conditions of the account, Ms G is presumed liable for the loss in the first instance, in circumstances where she authorised the payments, and I think she did here. However, good industry practice was that Halifax ought to have been on the look-out for transactions that were unusual or uncharacteristic to the extent that they might indicate a fraud risk. On spotting such a payment instruction, I would expect Halifax to intervene in a manner proportionate to the risk identified. This is something Ms G's representatives said it should have done here, and it

thinks a proportionate response would have been for it to restrict Ms G's account. So, I have looked into this further.

Should Halifax have recognised at any stage that Ms G was at risk of financial harm?

The Financial Conduct Authority and Action Fraud published warnings about cryptocurrency scams from 2018 and, by the time this scam occurred in 2023, it was widely understood that there were associated risks in relation to payments made to cryptocurrency exchanges. So, I think, based on all that I said were Halifax's obligations, in addition, it ought to have been on the lookout for this scam occurring, and have an understanding as to what was at stake here. I do agree with Ms G's representatives that the risks associated with these sorts of payments, at the time they were made, were higher.

That said, from the outset, the circumstances with which Ms G approached transferring money out of her account with Halifax were different, from what she had tried previously, and this, I think, would have made it trickier for Halifax to identify when it ought to have stepped in here. I say this because, I think an earlier intervention and subsequent restrictions from the third-party bank, made Ms G change tact regarding how she was going to transfer money from her Halifax account and move her money out, and into the hands of the scammer.

So, even though Ms G was looking to transfer larger amounts from her Halifax account to her cryptocurrency account, and then to the scammer, I think she decided to make smaller, regular payments, to try not to trigger Halifax's fraud detection systems or alert it to make an intervention. I say this after reading the conversation that Ms G had with the scammer during the period of time relating to these payments.

On 29 June 2023, Ms G said to the scammer "If I hadn't moved bulk amounts quickly, it wouldn't [have] happened. I need to stay low for a while then I can start." And later on, in the scam on 13 September 2023 she said, "I will take a 30-minute break before I transfer from bank, 2000 left to transfer now." To which the scammer replied, "are you worried about being restricted by the bank?". Ms G then replied back "This is a true fact." And "Yes you know the last time my account was frozen for a month. This time I am doing it with all your support."

When I read the many messages between the scammer and Ms G over this period of time, I can see that she was getting coached to make payments with an aim to not alert Halifax or get an intervention from it. So, from the outset, Ms G and the scammer made it difficult for it to intervene here, and subsequently it didn't do so.

That said, I think even with what I have just concluded in mind, there was enough of a pattern developing here that I think Halifax ought to have asked more questions from the 15th payment that Ms G made for £3,000. I think Halifax ought to have asked what the payment was for and what Ms G was looking to use the cryptocurrency for ultimately. She had made another payment for £1,500 on the same day, and I think this was out of character, based on her account usage up to that point. I think when I consider this, and that the two payments were going to a cryptocurrency exchange, Halifax ought to have intervened. I think if it had done this it would have then needed to provide a warning to Ms G.

I think for the reasons I have given, Halifax ought to have contacted Ms G and provided a warning that specifically gave some of the key features of cryptocurrency-based scams, and informed Ms G of issues such as how these sorts of scams work.

If Halifax had provided a warning of the type described, would this have prevented the loss Ms G suffered?

I have read all of Ms G's contact with the scammer and there was a lot to go through. Their contact over four months was extensive, and after reading through it all, I think it is clear to me that Ms G had been taken in by the scammer and throughout, she was under his spell. I say this because, at several stages when an intervention was happening, either through the third-party bank, the police or her family, she was still taken in by what the scammer said, and trusted their word, over the authorities, the bank or her family.

I have, in particular, carefully read the messages between them during the time that I have concluded Halifax ought to have provided a warning to her. There are several messages, where the scammer has told Ms G what to say, and how to get through an intervention. I've read enough that persuades me, on balance, that any intervention from Halifax during the period of time that Ms G was making the transfers, wouldn't have made her deviate from her course of action.

I have said this after reading the lengthy discussion between the scammer and Ms G but also after reading the earlier intervention from a different bank. Ms G's representative has pointed to this and said Halifax ought to have done the same here: carried out a warning and then off the back of this, restricted Ms G's account.

I have listened to the call between the third-party bank and Ms G from June 2023, and can hear clearly a fairly robust warning being issued to Ms G. The bank had identified who the scammer was, that their website was fake and told her clearly that she was being scammed. But this didn't stop Ms G from continuing to talk to the scammer and then take directions from him once again. I think this is quite a clear example of just how much Ms G was being influenced by the scammer here.

Addressing Ms G's representative's point about Halifax essentially doing the same as the first bank, and restricting her account, I don't, on balance, think the same scenario would have played out in the same way, if it had done what it should have done here. I say this, because I can see Ms G and the scammer were adapting to what had happened before. I have already given an example of how Ms G transferred over smaller amounts to try and not trigger Halifax's fraud detection system. I think by extension of this, based on what I've read, it is more likely than not, that she would have adapted her approach to any warning provided by Halifax too. She was being coached by the scammer to give certain answers, to avoid her account from being restricted.

I do appreciate that Halifax would have been more explicit with regards to tailoring its warning to a cryptocurrency investment scam, and some of those warnings could have rung true with what Ms G had involved herself in at that stage, but I don't think it would have been anything she hadn't heard before from the other bank earlier on in the scam. In addition, I think it is clear from the exchanges that I have read between the scammer and Ms G, that she was motivated to make the payments and ultimately most likely would have done so regardless of what Halifax had done in this case. In short, Ms G would have done what she needed to, to make the payments which she lost to the scam.

Was Halifax able to recover the funds once it found out about the scam?

Finally, I've thought about whether Halifax could have done more to recover the funds after Ms G reported the fraud. This is something in certain circumstances it would have been able to look at once it had been notified about the scam from her.

Ms G didn't make the payments to the scammer, instead she made them initially, to her own account on a cryptocurrency exchange. So, I wouldn't normally expect Halifax to attempt to claim back funds in these circumstances where the money was transferred to Ms G's own account with a business, who were carrying out a service for a legitimate purpose. In any

event, by the time Ms G notified Halifax she'd been scammed, the funds had already been sent onto the scammers in the form of cryptocurrency which wouldn't reasonably have been something Halifax could have successfully recovered.

In summary

I've read an extensive number of documents about this scam and having done so I'm sorry about what has happened to Ms G. It is clear to me that she was cruelly scammed over a prolonged period by a criminal and lost her money despite interventions from the third-party bank and the authorities. But even with that being said, in conclusion I can't fairly tell Halifax on this occasion to reimburse her, in the circumstances that I have described.

I'm not persuaded any intervention would have caused Ms G to have not gone ahead with the payments. I also don't think Halifax had an opportunity to recover her funds.

My final decision

My final decision is that I do not uphold Ms G's complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms G to accept or reject my decision before 8 August 2025.

Mark Richardson
Ombudsman