DRN-5072951

The complaint

Mrs G complains that HSBC UK Bank Plc didn't do enough to protect her when she fell victim to a cryptocurrency investment scam.

What happened

In Summer 2021, Mrs G received a cold call about investing in what she recalls was "stocks, shares and cryptocurrency". She began investing in August 2021 through her HSBC debit and credit cards and then from September 2021 until January 2023 she made faster payments online to a new account in her name with an electronic money institution ("EMI"). From here, the scammer guided Mrs G to invest the funds, mostly via cryptocurrency exchanges. In total, Mrs G sent £203,138 by faster payments to the scam.

In January 2023, the scam was revealed when Mrs G's family member saw someone had accessed their business account and taken funds. Mrs G reported the scam to HSBC and initially explained that she hadn't authorised the payments. HSBC didn't uphold her complaint and said its evidence indicated the payments were authorised by her, or at least by someone with her consent.

Mrs G came to our service and our Investigator partially upheld her complaint. At this time, it's accepted Mrs G is the victim of a scam and I've seen there is an FCA warning for the firm she paid. It's now also been accepted that, albeit under the spell of the scam, Mrs G did authorise the payments out of her account. Our Investigator considered HSBC should've intervened by phone on the first faster payment Mrs G made as it was out of character for her. He believed this phone call should've prompted HSBC to ask Mrs G into branch and the scam would've unravelled. But he also said Mrs G should share responsibility for her losses.

I attempted to mediate this case before issuing a final decision. I agreed with our Investigator's assessment and set this out to HSBC. It disagreed that it should be liable when the EMI wasn't. And after some conversation, said it wasn't persuaded a branch visit would've been prompted by the call, but had it occurred, it wouldn't have prevented the losses. As no agreement could be reached, I've reviewed the case to issue 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.

I've considered longstanding regulatory expectations and requirements, and what I consider to be good industry practice for firms when processing payments. In line with this, HSBC ought to have been on the look-out for the possibility of fraud and made additional checks before processing payments in some circumstances.

Looking at 12 months of Mrs G's statements prior to the scam, her account runs with a fairly common and nominal balance until January 2021, when she receives a very large credit from an equity release. By March 2021 the vast majority of this money has been moved, over 50% of it by one cheque payment, and by mid-April 2021 the account balance is under

£10,000. This amount is gradually spent between April and August 2021, when the scam starts.

On 1 September 2021, Mrs G's account is in overdraft by just over £2,000 until money credits the account from the pension cashed in to fund the large scam payment about to be made. Mrs G then, with the help of the scammer, arranges an online payment for £25,000 to be moved to her newly opened account with an EMI.

The information HSBC held was that a large, out of character payment was made online to a new payee, which was an account with an EMI. The amount of the payment was high, it's over double what the running account balance had been for five months on the account; and previously payments of this nature have either been made by cheque or to well-known and established recipients, such as HMRC. The payment was also funded by two credits received to the account the same day from a company where the consumer must have held either a pension or investment/s. I consider HSBC ought to have been concerned by this and contacted Mrs G. It's confirmed that concerns about outbound payments were always investigated by telephone, so based on this, I consider it should have called Mrs G at this time.

I recognise Mrs G did send payments to the scam prior to this one, some using her credit card and others on her debit card. But having considered when they were made, their value and who they were made to, I'm not persuaded HSBC ought to have found any of those payments suspicious, such that it ought to have made enquires of Mrs G before processing them.

HSBC didn't contact Mrs G about the 1 September 2021 payment – or in fact any payments until 2023. This means I have to make a decision on what's most likely to have happened if it had done what it should have in 2021. I recognise that in some situations a phone call intervention, or even several phone calls would've made no difference to the chain of events. But in this case, I consider it's more likely a phone call actually would've changed the chain here – and stopped the losses. I'll explain why.

In 2023, 18 months after Mrs G starts this "investment" opportunity, HSBC does call regarding a payment. Listening to the call, Mrs G doesn't sound confident on the phone. There are very often long pauses between the question asked and the answer given, including for things she should clearly and quickly know. She isn't clear about whether the payment was made by her mobile banking or online, despite the fact she had very recently made it. And the conversation doesn't flow as you'd expect.

There's also feedback and other noise at times which, while I appreciate is with the benefit of some hindsight, I'm persuaded is from the scammer being on another phone. In the call the advisor is clear he's struggling to hear Mrs G several times and she struggles to hear him too. Despite the scammer being there to coach Mrs G, when asked why she is making the payment she says she's *"possibly buying bitcoin"* and then also says she is moving funds to use the Revolut account more. And she also mentions she's received some of the funds he questions from someone else (even though they come from her own account). And around 20 minutes into the call she shares that a friend is helping her. None of this is queried by the advisor.

So while Mrs G was being coached, she still revealed core information about the scam that HSBC could and should've picked up on – especially in 2023, when these scams were far more prevalent. I recognise it's impossible to know exactly how a call would've gone in 2021, or what information Mrs G would've shared at this time. But as above, that means I have to decide what's most likely to have happened.

During the call in 2023, 18 months into the scam, Mrs G doesn't seem confident on what to say or what was going on. She wasn't either willing or able to confidently mislead the bank about the payments. From what I've seen of these kind of scams, most individuals are coached to conceal that they're buying cryptocurrency and that any other party is involved/helping them, whereas Mrs G openly shared this information. Unfortunately her recollections of the scam are limited due to both her age and health, so we can't establish now if she shared this against the scammer's advice or not.

HSBC has argued it would be "highly unusual" for a customer to be asked to come into branch regarding an outbound payment. But this is a highly unusual situation. I recognise HSBC is not expected to give financial or investment advice, or to protect its customers from poor investment decisions. However it should respond to the information it does hold and act proportionately where there is a heightened risk of financial harm from fraud.

Had HSBC called Mrs G, I'm confident she'd have shared that the funds came in from her pension. I can see she shared this with the EMI around this time, when asked. And it seems likely, based on what was openly shared in 2023, Mrs G would've explained she was looking to invest in bitcoin and was receiving help – which I think ought to have raised concern about the risk she could be falling victim to a scam.

In any event, if she hadn't shared about bitcoin and had instead shared that she wanted to *"use her Revolut account more"*, as this is the other reason she gave in 2023, this still ought to raise concern. It should still be a red flag that someone claiming on a pension, would cash-in this long-term investment, to simply increase their account usage with an EMI. I think this ought to have warranted further questioning from HSBC. And, based on her call in 2023, I'm not persuaded it's likely Mrs G would have been able to maintain an audibly plausible, persuasive cover story for why she was doing this.

It is of course entirely possible that a customer could be genuinely looking to diversify and modernise their accounts and investments. But looking at Mrs G's profile, a pensioner who previously made large payments by cheque – this would seem quite a drastic change.

Mrs G has described the scammer's frustration at her limitations with technology and we hear her lack of confidence on the 2023 call. She wasn't able to answer simple questions, such as why or how she made the payment that day without hesitation (likely reverting back to the scammers). Given how much control they had over the investment, I consider it likely she would have come across similarly confused if questioned earlier into the scam – when she had even less knowledge about the scheme.

I'm also conscious that, even with the coaching, Mrs G divulged that she was considering purchasing cryptocurrency based on third-party involvement. I therefore think that, if HSBC had called her in September 2021, it would likely have had concerns – both about the scam risk, and about her lack of understanding about what she was doing. There's a vulnerability that can be heard in the 2023 call, through both Mrs G's demeanour and conversation flow. In those circumstances, I think the proportionate response would have been to call her into branch for an in-person conversation.

HSBC argues that had it asked Mrs G to come into branch, the scammer would've taken the time to heavily coach and prepare her. On one hand, this is possible – and I do accept likely. But I do also consider there's an alternative here where, due to Mrs G's vulnerabilities and lack of understanding, they may also have cut their losses at this time. As above, Mrs G's testimony details the scammers frustrations with her and her limitations – so there is a possible situation where they accept that coaching is unlikely to work and end contact.

However, we don't know this and considering Mrs G had just cashed in her pension, it's

equally, if not more likely, the scammer would try and coach Mrs G just in case it paid off. But as above, I'm not persuaded that she would've been able to persuade branch staff she was sending the funds to the EMI for any legitimate reason – and/or that she was independently investing in bitcoin.

Once the scam came to light, Mrs G didn't know how to access the cryptocurrency accounts used to get evidence from them, or check if any funds remained. We understand she used screensharing software with the scammer so they could carry out some actions on her behalf and coach her through others. So the scammer would've needed to convince Mrs G to mislead HSBC entirely about the purpose of the funds *and* on how to persuasively do so, had she not already revealed the true purpose. *Or* to actually teach Mrs G enough about cryptocurrency investing – so she could've persuaded HSBC she was doing this herself/with a trusted personal friend. The scammer was of course not a regulated broker, so a reveal of their involvement as a firm would've been a concern.

Reviewing the evidence we hold, I am not persuaded the scammer could've done either of these things considering the likely time scales and Mrs G's personal characteristics and technical understanding. It's also important to remember that I consider this branch visit should've happened only a month into the scam, when Mrs G was still new to the opportunity and so while I accept she was convinced by it, she didn't have a large financial or emotional investment in the opportunity.

I'm persuaded that had Mrs G come into branch for an in-person conversation with HSBC, the scam would've unravelled, as she wouldn't have convinced the staff she wasn't at high risk of financial harm if it allowed the payment to be processed.

Our Investigator set out about the Banking Protocol and how HSBC could've invoked this if needed. This was well established by 2021 and designed for situations like Mrs G's. So the staff in branch should've been trained to look out for the signs Mrs G was falling victim to a scam and acted to protect her. I'm also not persuaded that Mrs G would've been confidently able or willing to lie to the Police had they got involved, considering this was a new venture and she had little understanding about the investments she was making. So had the Banking Protocol been invoked, I'm confident the scam would've unravelled.

Due to everything I have outlined above, I'm persuaded it's most likely that had HSBC called Mrs G about the £25,000 payment on 1 September 2021, this would've unravelled the scam at this point. This means that this payment wouldn't have been made and all subsequent payments to the scam not made, or lost.

Contributory negligence

As both parties are aware, I also need to consider if it's fair for Mrs G to hold some responsibility for her losses in this case. And I'm in agreement with the Investigator that it would be fair to do so here.

I accept Mrs G's vulnerabilities and that she's been the victim of a cruel scam. But I consider there were red flags for her to see as well as the bank. I understand she was cold called about this opportunity and then allowed this company access to her devices and banking, and she's admitted to leaving her devices unattended while knowing they had access.

On their advice, Mrs G cashed in existing long-term savings and investment plans to invest in something she didn't fully understand and wasn't being asked to understand. The scammer took control rather than educating Mrs G on the opportunities. Remote access and not caring if the customer understands the products are not behaviours you'd expect of a legitimate firm. And as Mrs G did have relationships with other investment firms, she had

comparators for their behaviour. Mrs G also didn't receive the same kind of paperwork she held with the other firms or have any credentials for the scam firm, which should've been another concern. So I do think she contributed to her losses in this case.

Putting things right

Mrs G sent £203,138 out of her HSBC account to the scam from 1 September 2021 onwards, when I consider the losses could've been prevented.

However, when the scam was uncovered, £7,237 was recovered from Mrs G's EMI account from the final £14,000 payment she sent from HSBC, so this amount was not lost, effectively reducing this payment to £6,763. This makes her actual loss £195,901.

HSBC UK Bank Plc should refund Mrs G 50% of each of the payments she made to the scam from 1 September 2021, which will total £97,950.50. It should pay 8% simple interest per anum on these payments from the date of payment to the date of settlement.

My final decision

For the reasons set out above, I partially uphold Mrs G's complaint against HSBC UK Bank Plc.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs G to accept or reject my decision before 10 January 2025.

Amy Osborne
Ombudsman