DRN-6241552

The complaint

Mrs W and Mr W complain HSBC UK Bank Plc ('HSBC') won't refund the money lost after Mrs W fell victim to an authorised push payment ('APP') scam.

The complaint has been brought with the assistance of a professional representative. Whilst the account is a joint account, I understand the account is solely used by Mrs W and, it was Mrs W who made the payments in question. So, for ease of reading, I will refer to her throughout this decision.

For completeness, I'm aware Mrs W made a payment in October 2023 which was raised under a separate scam claim. While this might be referred to for the purpose of setting out the wider circumstances and in explaining the findings reached, I make no findings in relation to this payment.

What happened

Both parties are aware of the circumstances of the complaint, so I won't repeat them all here.

In or around October 2023, Mrs W received a message from a third party via a well-known messaging app. The message was intended for a different individual and not Mrs W. The message received was in a language Mrs W is fluent in, and she and the third party continued to message each other. I understand a romantic attachment then developed.

The third party shared with Mrs W that he made money investing in cryptocurrencies, alongside his relatives. Believing the third party, Mrs W decided to invest and between 27 November 2023 and 20 January 2024, she made five payments totalling £50,000.

Mrs W was sent a link to download an app – which I'll refer to a 'F'. After downloading F, Mrs W contacted customer service via F and was provided with the account details to transfer the funds to. These would then credit her account with F.

In order to fund some of the later payments Mrs W made, she borrowed funds from two friends.

When she attempted to make a withdrawal of her funds, she was told she'd need to deposit more money. Mrs W visited family abroad and says it was when speaking to them that they advised her this was a scam.

Mrs W subsequently contacted HSBC in February 2024 to raise a scam claim. It investigated the matter but declined to refund the money Mrs W had lost. HSBC considered the payments Mrs W made under the Lending Standards Board's Contingent Reimbursement Model ('CRM Code'). It said both HSBC and the beneficiary bank had sufficient fraud prevention measures in place, however, Mrs W could have taken more care and carried out more checks before sending the payments. HSBC added that a fraud warning was provided to Mrs W at the time of the payments and she'd reported to the bank that she hadn't read this warning. It held Mrs W liable for the payments as she was contacted out of the blue by a

third party and whilst a relationship had formed, she didn't complete any checks on the payments she was making, didn't receive any paperwork about the investment and didn't question why the payments were going to a person.

Mrs W wasn't happy with HSBC's response, so she brought a complaint to our service.

An Investigator looked into Mrs W's complaint but didn't uphold it. In brief, she thought HSBC had established a valid exception to reimbursement – she didn't think Mrs W had a reasonable basis for belief when making the payments. Our Investigator acknowledged Mrs W had been identified as a victim of fraud in the weeks prior to the five payments she made and so, thought HSBC was on notice that Mrs W was at risk of financial harm from fraud. She said, given the size of the payments, the prior scam history, that the payments were to a new payee and the confirmation of payee result ('CoP') was a no match, it ought to have prompted HSBC to have intervened further than a written warning. Our Investigator concluded HSBC ought to have provided a human intervention. However, when considering the specific circumstances she didn't think further interventions would've made a difference and prevented the loss. It followed that she didn't recommend HSBC reimburse Mrs W the money she'd lost.

Mrs W disagreed with the Investigator's opinion. In summary, but not limited to, she said:

- HSBC had already identified she was a scam victim in October 2023. From that moment, the bank was not dealing with a hypothetical risk, it had clear confirmation that she was actively being defrauded. This placed HSBC under a significantly heightened duty to safeguard her from further harm.

- Once the bank knew that she was vulnerable and subject to manipulation, relying solely on automated warnings was inadequate and fell short of the standards expected under the CRM Code.

- The conclusion that such intervention would not have had a material impact is speculative and inconsistent with the purpose of the CRM Code, which expressly emphasises the importance of real-time human engagement in interrupting scams particularly where undue influence is suspected.

Our Investigator considered the further points, but her conclusions remained unchanged. She accepted HSBC ought to have intervened, including providing a human intervention. However, she noted that HSBC had already advised Mrs W, during an earlier payment, that she had been the victim of a scam and had raised a scam claim on her behalf. Despite this, Mrs W attempted another payment from an account she held with a different payment service provider and later transferred funds from an account she held abroad.

Further, even after Mrs W's family told her she had been the victim of a scam, she continued communicating with the third party. Because of this, our Investigator didn't think a better warning or intervention from HSBC would have prevented the loss. The Investigator also considered vulnerability under the CRM Code but did not think the circumstances met the high bar required. She noted that Mrs W herself questioned the investment's legitimacy and said she knew little about the third party.

Mrs W still disagreed and asked for an ombudsman to review her case.

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.

Firstly, I'm aware Mrs W made a payment of 200,000 HKD, from an account she held abroad. As our Investigator explained, we are unable to consider this payment. The Dispute Resolution Rules (DISP Rules) 2.6.1 outlines that compulsory jurisdiction covers activities of firms that are carried out from an establishment within the United Kingdom ('UK'). Given the payment was made from Mrs W's account which she held in a different country – this is outside of the UK and our jurisdiction.

In deciding what's fair and reasonable in all the circumstances of a complaint, I'm required to take into account relevant: law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to have been good industry practice at the time.

I'm sorry Mrs W has been the victim of a scam, and I don't underestimate the impact it's had on her. I realise it is a significant amount of money she has lost and so, I understand why she is doing everything she can to recover it. But just because a scam has occurred doesn't mean Mrs W is automatically entitled to a refund by HSBC. It would only be fair for me to tell HSBC to reimburse Mrs W if I thought they were responsible for her loss. Having carefully considered this, I don't think HSBC has acted unfairly by not providing a refund. I'll explain why.

Before I do, I want to reassure Mrs W that I've considered everything that has been submitted in support of her complaint. While I've summarised this complaint in far less detail than what has been provided, I want to stress that no discourtesy is intended by this. If there is a submission I've not addressed; it isn't because I have ignored the point. It's simply because my findings focus on what I consider to be the central issue in this complaint – that being whether HSBC are responsible for any loss Mrs W suffered because of the scam.

In broad terms, the starting position at law is that a firm is expected to process payments and withdrawals that a customer authorises, in accordance with the Payment Services Regulations (in this case, the 2017 regulations) and the terms and conditions of the customer's account.

It's not in dispute that Mrs W made the scam payments. So, the payments were authorised and under the Payment Services Regulations, the starting position here is that Mrs W is responsible for the payments (and the subsequent loss) despite the payments being made as the result of a scam.

However, that isn't the end of the story. At the time Mrs W made the scam payments, HSBC was signed up to the CRM Code, which was in place until 6 October 2024. The CRM Code provided additional protection to consumers who had been the victims of APP scams like this, in all but a limited number of circumstances.

Not all scam payments covered by the principles of the CRM Code are required to be reimbursed. Under the CRM Code there are exceptions to reimbursement. Relevant to this complaint is R2(1) of the CRM Code, which states:

> *"A Firm may choose not to reimburse a Customer if it can establish any of the following matters in (a) to (e). The assessment of whether these matters can be established should involve consideration of whether they would have had a material effect on preventing the APP scam that took place…*
>
> *(c) In all the circumstances at the time of the payment, in particular the characteristics of the Customer and the complexity and sophistication of the APP scam, the Customer made the payment without a reasonable basis for believing that:*

(i) the payee was the person the Customer was expecting to pay;

(ii) the payment was for genuine goods or services; and/or

(iii) the person or business with whom they transacted with was legitimate…"

I've carefully considered Mrs W's testimony and the evidence she's provided of the scam. I'm really sorry to disappoint Mrs W, but I think a valid exception to reimbursement applies in this case, specifically that Mrs W made the scam payments without a reasonable basis of belief. I say this because;

- Mrs W was contacted by the third party out of the blue who was claiming to be sending a message to someone else. I appreciate the third party was communicating in a language Mrs W was fluent in and that they continued to speak with each other – with contact becoming frequent. While I accept that a romantic relationship formed between them, during the communication Mrs W did ask the third-party questions to get to know them better and acknowledged at points that she didn't know much about the third party. Yet, she seems to have trusted what the third party had told her about his success with investing in cryptocurrencies and the payments she was making. It's been said Mrs W downloaded F via a mobile device store, but she received a link from the third party to download F via the messaging app. Given that the app was sent via a link from someone that she hadn't long known, I think ought to have led Mrs W to proceed with more caution than she did.

- It was via F's customer services that payment details were provided. The account details for the payment Mrs W made in October 2023, while not one of the five payments she made that are being considered under this complaint, was given to her via F. When there were issues with this payment – Mrs W being told the funds hadn't been received by the beneficiary, Mrs W contacted HSBC. At this time, an agent of HSBC told Mrs W that this looked like a scam itself. They added that they'd searched the app – F – and it didn't seem like a genuine company. The agent reiterated that it wasn't a genuine app – it was a scam. The agent provided Mrs W with information around carrying out independent checks and the Financial Conduct Authority ('FCA') website, amongst other things. Mrs W shared that she didn't think it was F that was the scam but the account she paid – which for the payment in October 2023 was a business account. The subsequent payments Mrs W made were to an individual. I've thought carefully about this, but I think this ought to have been a red flag to Mrs W. She was told in the call with HSBC's agent that the app (F) was not genuine after being searched. Looking at the chat messages between Mrs W and the third party, I can't see that she raised this with them. She didn't question what the bank had told her about the payment she'd made with the third party she was speaking with. From the chat messages the third-party informed Mrs W that he'd sent the funds back to her and these were reinvested.

- Mrs W subsequently went on to send several payments to the account details she received from the customer services of F. I think Mrs W ought fairly and reasonably to have asked more questions about what she was being asked to do. I understand Mrs W had developed feelings for the third party but I'm also mindful she'd been told she'd fallen victim to a scam in relation to a payment she made in connection with F, and this was the same app Mrs W was still using. So, I think this ought to have caused her concern and prompted her to ask further questions about F, the account she was being asked to pay and of the third party.

- Within the communication between Mrs W and the third party, I note that there were times when Mrs W didn't appear fully comfortable with what the third party was asking her. For example, when the third party encouraged her to borrow funds from friends and family and when she was directed to open up an account with another provider. I'm mindful Mrs W ultimately doesn't appear to have opened up the account she was asked to and that for a period of time she pushed back on asking friends for money. However, she later did go on to borrow funds from friends to invest. I think this indicates that Mrs W wasn't fully happy with what she was being asked to do and she also appears to have recognised that she didn't know too much about the third party as a person.

- Within the chat messages, I've not seen that Mrs W was coached about what to say, but she's shared that she was told not to discuss the investment with anyone as it was internal information. I think this ought to have caused Mrs W some concerns.

- Around 3 January 2024, Mrs W told the third party she'd soon be visiting family and that she may need to withdraw some funds from F to use. She asked how long this would take to process. I can't see that Mrs W received a response to her questions, instead she received a message about preparing the funds and the third party's belief that Mrs W could do it. Mrs W replied to say that the third party kept asking her to invest money, and more and more and that this made her feel so much pressure to make money. Around the same time, Mrs W said *'you always ask me to do things that I am not willing to do, and I always give in, but what about you?...'* On balance, I think this indicated that Mrs W had doubts about what she was being asked to do by the third party and ought fairly and reasonably to have given her pause for thought. Especially given that when she asked about making a withdrawal - she either didn't receive a response or was being told 'sure' she could make a withdrawal and would be shown how to it but hadn't successful withdrawn any funds.

- Overall, I've seen no evidence that Mrs W attempted to verify the third party, the company, or F (the app), or to check their legitimacy or expertise.

While I don't ignore the fact Mrs W believed she'd developed a relationship with the third-party, given that she herself expressed that she didn't know too much about them, given all the other factor's I've shared above, I can't safely say Mrs W had a reasonable basis for belief, when making the payments.

I acknowledge the comments around Mrs W being groomed and manipulated in the context of a long-term romance scam, but I have to be mindful that Mrs W started speaking with the third party around October 2023 with payments under this complaint starting from November 2023. Given this, Mrs W and the third party had been communicating for a few weeks and so, I don't find I am able to consider this a long-term romance.

Effective warnings

I've gone on to think about whether HSBC did what was expected of it at the time Mrs W made the payments. Good industry practice requires that regulated firms such as HSBC engage in the monitoring of customer accounts and to be on the lookout for suspicious or out of character transactions with an aim of preventing fraud and protecting customers from financial harm. And under the CRM Code, where it identifies a risk of a customer falling victim to an APP scam, it is required to provide that customer with an "effective warning".

Having done so, I'm in agreement with our Investigator and for much of the same reasons. Given that HSBC had identified Mrs W had fallen victim to a scam in early November 2023, I

think it was on notice that Mrs W was at risk of financial harm from fraud. I do note that the subsequent payments Mrs W made were to a new payee – an individual and not a business, as with the previous payment but given the size of the payments, that the payments were to a new payee and that there was a CoP no match, I think this ought to have prompted better intervention. HSBC provided a written warning based on the payment purpose Mrs W selected – 'buying goods or services'. In light of the above factors, I'm persuaded HSBC ought to fairly and reasonably have contacted Mrs W to discuss the payments she was asking to make. This said, I'm not persuaded that a better warning or intervention in this case would've prevented Mrs W's loss. I'll explain why.

From the chat messages provided to us, I can see Mrs W and the third party were frequently speaking – throughout the day, and Mrs W was sharing aspects of her life with the third party. While I note Mrs W raised questions at points – even expressing at times she felt pressured, I have to keep in mind that she ultimately moved passed these feelings and went on to borrow funds from friends for example. As such, I think this showed Mrs W was under the third party's spell.

I also can't ignore that Mrs M attempted and sent payments from other accounts – such as from an account she held abroad. I think this show's Mrs W had the means and determination to make the payments. Payments which were made after HSBC had informed her a payment she made in October 2023 in connection with F was a scam.

Further, I can see in February 2024, Mrs W shared with the third party that her family members had all said she'd been scammed and after blocking the third party she went on to unblock him and sent him further messages.

So, even if HSBC had called Mrs W and explained why it thought she was the victim of an investment scam, I'm not satisfied I can fairly say it's more likely than not that Mrs W would've believed HSBC over the third party. It's possible that it would've given her pause for thought, but I think she would have more likely than not proceeded to make payments.

I realise that I'm making a conclusion on what I think Mrs W's actions would've been in a hypothetical situation. However, I only have to reach a decision on the balance of probabilities. In other words, what I think would more likely than not have happened based on the available evidence.

In this case, I'm not convinced that HSBC talking to Mrs W about the payments would've broken the spell the third party had her under or meant that she wouldn't have continued with making payments.

Vulnerability under the CRM Code

There has been reference to Mrs W being vulnerable. I've carefully thought about what's been shared with us. The CRM Code says that there are provisions which might lead to a refund, even when a customer doesn't have a reasonable basis for belief. The relevant part of the CRM Code says:

> *'A Customer is vulnerable to APP scams if it would not be reasonable to expect that Customer to have protected themselves, at the time of becoming victim of an APP scam, against that particular APP scam, to the extent of the impact they suffered.'*

So, I've considered whether there were vulnerabilities present at the time to such an extent that Mrs W was unable to take steps to identify the scam she fell victim to or to recognise steps she might take to test the legitimacy of what she was being told by the scammer. To

do so I must consider the details of the scam, Mrs W's actions throughout, and the wider circumstances of what was happening.

On balance I think there is evidence within the circumstances that suggests Mrs W was capable of taking steps to protect herself from fraud and financial harm. That is to say there was more she might reasonably have done that would have led to the scam being uncovered.

Mrs W – at points questioned what she was being asked to do with the third party. At one point she was asked to open an account with another payment service provider – I'll refer to as W. She expressed she wasn't happy to do this and ultimately, from what I've seen didn't proceed to open an account to make payments as part of the scam.

Further, I can't ignore the call between Mrs W and HSBC in early November 2023, in which the agent informed Mrs W that the payment in question (a payment Mrs W made in October 2023), looked like a scam - the agent mentioned the app itself – F which they said they'd searched online and didn't seem to be a genuine company and the name given to make that payment to was a different person to the company name. During this conversation with the agent, Mrs W seems to realise it was a scam. The agent provided advice on checks to be completed, such as Mrs W checking the FCA website, to do independent checks and to contact the company on verified details, amongst other advice. Again, Mrs W within this call seemed to acknowledge what the agent had told her.

Yet, following this, Mrs W appears to have continued to make payments in connection with F – who was sending the account details for the payments. Mrs W doesn't appear to have undertaken any of the checks recommended by the bank and, I've not seen anything that suggests there was a reason Mrs W was unable to do so.

Based on everything I've seen and been told, I don't think it's unreasonable to have expected Mrs W to have carried out research and, importantly, I've not seen any evidence to suggest that it would be unreasonable to have expected Mrs W to have done this and in doing so protected herself from the particular scam she fell victim to. I've not seen any evidence to suggest Mrs W didn't have the capacity and understanding to query the legitimacy of what was being offered.

Whilst I've carefully thought about the wider circumstances – her separation a few years prior and the financial responsibilities that followed, overall, I'm not satisfied these aspects demonstrate that Mrs W couldn't have protected herself from the scam she fell victim to. And, as a result, I don't think she is entitled to reimbursement under the CRM Code.

Recovery

Finally, I have considered whether HSBC did all it could to try and recover the money Mrs W lost.

Mrs W raised the scam payments with HSBC on 15 February 2024, which was several weeks after the last payment was made on 20 January 2024. So, it was unlikely that there would have been a realistic prospect of success with any recovery attempt. Sadly, it is common for fraudsters to withdraw or move the money on as quickly as possible.

All things considered, I don't find that HSBC is liable to refund Mrs W under the terms of the CRM Code. In saying this, I want to stress that I am very sorry to hear about what happened to Mrs W and I am sorry she has lost out here. She was the victim of a cruel scam designed to defraud her of her money. I appreciate that she's lost out because of what happened.

But I can only look at what HSBC was and is required to do and I'm not persuaded that HSBC is required to refund her under the CRM Code, nor that the bank was at fault in making the payments Mrs W had instructed it to make or for any other reason.

My final decision

My final decision is that I don't uphold this complaint against HSBC UK Bank Plc.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs W and Mr W to accept or reject my decision before 8 May 2026.

Staci Rowland
Ombudsman