DRN-4204761

The complaint

Mrs E complains that HSBC UK Bank Plc won't reimburse her for the money she lost when she fell victim to an 'authorised push payment' ("APP") safe account scam.

What happened

I issued my provisional decision on this complaint on 30 March 2023. The background and circumstances to the complaint and the reasons why I was provisionally minded to uphold this complaint in part were set out in that decision. I've copied the relevant sections from that provisional decision here, and it forms part of this final decision.

The detailed background to this complaint is well known to both parties and I'm mindful that it is difficult for Mrs E to have to recollect all of the details of what she has been through. Our Investigator has captured the events in detail in her view, so I have only outlined the key elements to the background here.

In early 2021, Mrs E made a connection through a well-known social media platform's dating application, to a person I'll refer to as B, but unknown to her at the time B was a fraudster. Between January 2021 and March 2021, the fraudster persuaded Mrs E to make international payments to help him, while he was working on a project abroad. B's reasons, for why the money was needed, escalated from needing money for food, having to pay tax to local authorities, through to being kidnapped and needing money to pay off a gangster, who B said was threatening his life. During this time, Mrs E made a number of international payments, through an account she held with another bank, resulting in her losing over £35,000.

In early March 2021, Mrs E attempted to make a further payment for £30,000 from the account she held with the other bank. But the bank, suspecting she was the victim of fraud, refused to make the payment and invoked the Banking Protocol. As a result, on 5 March 2021, Mrs E instead transferred the £30,000 to her HSBC account (by way of two transfers for £15,000), with Mrs E telling her other bank she wouldn't be using the funds to send abroad, but instead would use it to repay loans she had taken out.

But, at this point, Mrs E was still under the spell of the fraudster, and she believed B's life was at risk. He'd told her he was being held against his will by a gangster, from whom he had borrowed money and he needed to pay the gangster £30,000. Mrs E has acknowledged she lied to her other bank and to the Police, after the other bank had invoked the Banking Protocol, telling the Police that everything was ok.

Despite what she'd been told by her bank, about its concerns about her being scammed, Mrs E still believed she had to get money to B, to pay the gangsters and save his life. B had asked Mrs E to send money to his interpreter, his interpreter's wife and to his housekeeper/carer, so that they could forward it on to him, in Eastern Europe. Still under the spell of the fraudster Mrs E made the following payments from her HSBC account;

3 March 2021	*£4,000*	*(international payment to interpreter)*
5 March 2021	*£12,000*	*(UK payment to housekeeper/carer)*

5 March 2021	*£8,000*	*(UK payment to housekeeper/carer)*
5 March 2021	*£10,000*	*(international payment to interpreter's wife)*

HSBC's fraud detection systems blocked the payments for £10,000 and £8,000, and it asked Mrs E to call it to discuss the payments. Mrs E told HSBC the £8,000 was for her stepdaughter's carer for bills, and that the £10,000 was for her partner, who had been held up abroad, so had further accommodation costs. HSBC also questioned the other payment, for £12,000, that Mrs E had made to the carer on the same day. Mrs E told HSBC this payment was for a car for her stepdaughter. Following this call HSBC released the payments.

Mrs E has said B told her that he'd offered the £30,000 to the gangster, but they then demanded a further £15,000 in interest, and without this they wouldn't release his passport. Mrs E has said she was distraught by this point, but her sister agreed to raise the money, which her sister then sent to the housekeeper (the payments that Mrs E's sister made do not form part of this complaint).

A couple of days later, Mrs E has said that B told her that he was free. She's said that he told her he'd paid immigration some money for a fast-track Covid test and for an overnight stay and that he'd booked his flights back to the UK, sending Mrs E what appeared to be booking details for a flight on 16 March 2021.

Mrs E has said she went to the airport, expecting to pick B up. But shortly before the flight was due to land, Mrs E received an email from whom she thought was an airport official, saying that B had been arrested and was under investigation. Mrs E has said, with this, she spoke to UK border forces at the airport who told her the email was likely to be fake. Mrs E said she waited for over three hours at the airport, but B didn't arrive.

Mrs E then received another email from the airport official. It said B had helped somebody carry their luggage, but it had been found to contain illegal substances. The airport officials told Mrs E that although the other passenger had told them that B wasn't involved, they wanted money 'under the table' to enable B to fly home – they were asking for £55,000.

Mrs E has said she spoke to UK Border Force again, who told her she ought to call the Police. Having done so, she said the Police told her it was probably a scam email and that B would be on a later flight. But, while talking to the Police, Mrs E then received a call from B himself, who told her he was still being held abroad.

The following day, Mrs E received funds back for payments that she had tried to make to B from her other bank, but that had been returned by the beneficiary bank. Mrs E has said using this money, on 24 March 2021, she sent a further payment for £10,850 to the housekeeper, for them to send out to B. Mrs E has said she then raised further money, through her credit cards and borrowing from a friend.

Mrs E was then told by B to open a cryptocurrency account in her name. She's said she was under duress while doing this and she traded the funds where she was told to. Mrs E has said she thought this method would be an instant payment and help with B's release. Mrs E made the following payments into her cryptocurrency account, from here the money was sent to accounts that the fraudsters controlled;

26 March 2021	*£500*
26 March 2021	*£100*
26 March 2021	*£6,400*
29 March 2021	*£10,500*

With the exception of the payment for £100, HSBC blocked all of these payments and asked Mrs E to call it to discuss the payments. Unfortunately these calls aren't available.

Mrs E has said when B offered this money to the airport officials, they refused to accept it, as it didn't cover the amount that had been requested. B told Mrs E that as a result he was beaten up by officials and held in custody. But that if a further £10,000 could be raised, he would be set free.

Mrs E made arrangements to sell her car, to fund this payment. But later that day she went to visit B's daughter, at the address where B said he lived. But on arrival she was told that nobody by B's daughter's name, or the housekeeper's name, lived at this address. It was in this moment that Mrs E has said she realised she'd been scammed and called the Police. In total, Mrs E lost £62,350 from her HSBC account. A complete breakdown of the payments Mrs E made from her HSBC account is listed below;

3 March 2021	*£4,000*	*(international payment to interpreter)*
5 March 2021	*£12,000*	*(UK payment to housekeeper/carer)*
5 March 2021	*£8,000*	*(UK payment to housekeeper/carer)*
5 March 2021	*£10,000*	*(international payment to interpreter's wife)*
24 March 2021	*£10,850*	*(UK payment to housekeeper/carer)*
26 March 2021	*£500*	*(to cryptocurrency wallet)*
26 March 2021	*£100*	*(to cryptocurrency wallet)*
26 March 2021	*£6,400*	*(to cryptocurrency wallet)*
29 March 2021	*£10,500*	*(to cryptocurrency wallet)*

Mrs E contacted HSBC to report what had happened. HSBC investigated Mrs E's fraud claim and considered its obligations to provide her with a refund. HSBC is a signatory of the Lending Standards Board's (LSB) Contingent Reimbursement Model (CRM) Code which requires firms to reimburse customers who have been the victims of authorised push payment (APP) scams like this one in all but a limited number of circumstances.

It is worth noting here the CRM Code doesn't apply to all transactions made on a customer's account. Importantly, it doesn't apply to some of the payments Mrs E made as they were international payments; the Code only applies to payments made between UK based accounts. As well as this, the CRM Code only covers scam payments when the funds are being transferred to another person and not to a consumer's own account. With regards to the payments to the cryptocurrency accounts, Mrs E sent the money to her own account held with a cryptocurrency exchange. So the CRM code doesn't apply to the payments Mrs E made to international accounts, nor to the payments she made to her cryptocurrency account.

HSBC issued its final response on 8 July 2021, not upholding Mrs E's complaint. In summary it didn't think Mrs E had conducted any checks to validate the information that she was given was true or to confirm the person that she was dealing with was genuine. Alongside this, it considered it had provided sufficient fraud warnings. It understood that Mrs E considered herself to be vulnerable as she thought B's life was at risk, but it said when assessed under the CRM code, it wouldn't classify her position as vulnerable.

Unhappy with HSBC's response, Mrs E then brought her complaint to our service. One of our Investigators looked into things and didn't uphold Mrs E's complaint. In summary our Investigator explained that different considerations applied to the different types of payment she made. Regarding the international payments, our Investigator didn't think it was unreasonable for HSBC to allow the first international payment to go through, but that it was right to block the second international payment for £10,000 and to speak to Mrs E. But, while

our Investigator didn't think HSBC had asked enough questions during the call, she didn't think further questioning would have made a difference.

With regards to the payments Mrs E made to her cryptocurrency account. She thought it was reasonable for HSBC to block a number of these payments and to talk to Mrs E. Our Investigator noted that while she'd been unable to listen to these calls, she thought it more likely than not the conversations would have focussed on investment scams, rather than the type of scam Mrs E was falling victim to. Overall, she didn't think she could hold HSBC liable for these payments as, even if it had warned Mrs E or refused the payments, it was her view that Mrs E would have found another way to send the money.

For the three payments that Mrs E made to UK based accounts, our Investigator considered whether HSBC had been fair in not agreeing to refund these payments in consideration of the CRM code. In summary, our Investigator said she'd considered what Mrs E had said about making payments under duress and being vulnerable, but she didn't think she could be considered as vulnerable, as defined under the code. This was because it was our Investigator's view that, based on what she'd seen, there wasn't anything about Mrs E's mental or physical state, that would mean she would have been less able to protect herself from this type of scam.

Alongside this, our Investigator considered the warnings that HSBC said it provided during these payments. She didn't think either the online or verbal warnings could be considered as effective. But our Investigator couldn't see what HSBC could have done that would have made a difference. She said this because Mrs E had previously not accepted from her other bank, nor the Police, that she was being scammed.

Our Investigator added that she also didn't think Mrs E had a reasonable basis for believing the payments she made to the UK bank accounts were legitimate. She said this because Mrs E had been warned, in the strongest terms, by her other bank that she was a victim of a romance scam and it had refused to make payments. She had also received a visit from the Police and been told by multiple people, in positions of authority, that what was happening was probably a scam.

Overall our Investigator didn't think HSBC should refund the money Mrs E sadly lost.
Mrs E didn't agree with our Investigator's view. In summary she said;

- *HSBC has not followed the Banking Protocol or applied the appropriate level of care to protect her.*

- *Banks are there to protect vulnerable customers like her.*

- *Any assumptions about what she may have done, had the bank declined to make any further payments is irrelevant.*

- *HSBC didn't question the huge amount of borrowing.*

As agreement couldn't be reached the complaint has now been passed to me for a decision.

What I've provisionally 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 would firstly like to acknowledge how devastating it must have been for Mrs E to discover that she had fallen victim to such a callous scam. I understand her strength of feeling in pursuing this matter. But despite my natural sympathy for what has taken place, I can only uphold this complaint if I find that HSBC has not met its obligations in some way.

I'm mindful that in her submissions to us, after our Investigator had issued her view, Mrs E has said money was lent to her that shouldn't have been, which she went on to send to the fraudsters. If Mrs E wishes to complain about a financial institutions' lending decision, this is something she would have to take up with them in the first instance, to give them the opportunity to investigate.

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.

Under regulations, and in accordance with general banking terms and conditions, banks should execute an authorised payment instruction without undue delay. The starting position is that liability for an authorised payment rests with the payer, even if they were duped into doing so, for example as part of a romance scam. But, as well as the CRM code that I've mentioned, a bank also has wider obligations and a duty to protect its customers against the risk of fraud and scams so far as is reasonably possible. If, in breach of that duty, a bank fails to act on information which ought reasonably to alert a prudent banker to potential fraud or financial crime, it might be liable for the losses incurred by its customer as a result.

These transactions need to be dealt with in two parts; those made internationally and to Mrs E's cryptocurrency account (which are not covered by the CRM code) and then those made by faster payment to UK bank accounts (which are covered by the CRM code). That's because different considerations apply to the different types of payment, so I'll consider Mrs E's and HSBC's liability for each of these payment methods separately.

<u>The faster payments to UK bank accounts</u>

These payments are covered by the CRM code. The CRM Code requires firms to assess whether a customer was vulnerable to the APP scam they fell victim to at the time it occurred.

Mrs E has been brave enough to tell us something of her background, which I imagine was hard to do. These details have been shared with HSBC, so I don't feel the need to go into them in detail here.

I have considered what she's told us carefully. There is provision within the CRM Code for a customer to be reimbursed notwithstanding the exceptions to reimbursement, if the customer was vulnerable to APP scams and it would not be reasonable to expect them to have protected themselves against the particular scam they fell victim to.

HSBC didn't think there was enough evidence to prove Mrs E was vulnerable at the time of making the payments.

I've no reason to doubt Mrs E's submissions regarding her background; some of which is corroborated by Mrs E's counsellors, who, while mindful of patient confidentiality, have confirmed Mrs E as a patient, with them providing her with support around historical trauma. Mrs E's background recalls a horrific spiral of abuse, with roots back to her childhood, through to her adult life. While, in the moment Mrs E may not have recognised her own

vulnerabilities, when looking back I'm persuaded that the nature of this type of scam, preyed on and exploited the historic trauma that she had suffered.

Given what Mrs E has told us, I think these deep-rooted vulnerabilities would have impacted Mrs E's capacity to think clearly about the requests for payments while they were happening. I'm persuaded they made her more susceptible to falling victim to a scam of this nature and impacted her ability to protect herself. In short, I don't consider it would be reasonable to expect Mrs E to have protected herself against the APP scam she fell victim to at that time. I'm therefore minded to say that the fair and reasonable outcome here, when considering the CRM code, is that HSBC is responsible for reimbursing Mrs E for her losses covered by the CRM Code.

For clarity, this finding only relates to the three payments Mrs E made to UK bank accounts, as detailed below;

5 March 2021	*£12,000*	*(UK payment to housekeeper/carer)*
5 March 2021	*£8,000*	*(UK payment to housekeeper/carer)*
24 March 2021	*£10,850*	*(UK payment to housekeeper/carer)*

<u>The international payments and payments to Mrs E's cryptocurrency account</u>

As I mentioned earlier, the CRM Code doesn't apply to all transactions made on a customer's account. Importantly, it doesn't apply to the payments Mrs E made to international accounts, nor to the payments she made to her cryptocurrency account.

While I find the CRM Code doesn't apply here, it isn't the full extent of the relevant obligations that could apply in cases such as this. Taking into account the law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider HSBC should fairly and reasonably:

- *Have been monitoring accounts and any payments made or received to counter various risks, including anti-money laundering, countering the financing of terrorism, and preventing fraud and scams.*

- *Have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among 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.*

- *In some circumstances, irrespective of the payment channel used, have taken additional steps, or make 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.*

In this case, I need to consider whether HSBC acted fairly and reasonably in its dealings with Mrs E when she made the transfers, or whether it could and should have done more before processing them.

Did HSBC act fairly and reasonably when Mrs E made international payments and payments to cryptocurrency exchanges?

Mrs E has accepted she authorised the international payments and payments to her cryptocurrency wallet. Because of this HSBC had an obligation to follow her instructions. But there are some situations in which it should reasonably have had a closer look at the

circumstances surrounding the transfers - as I've explained, I consider that as a matter of good practice HSBC should've been on the lookout for unusual and out of character transactions.

Based on what I've seen I think the international payments, for £4,000 and £10,000, ought to have stood out to HSBC as not being typical of how Mrs E usually ran her account. So I think it would be reasonable to have expected HSBC to have sufficiently questioned her about these payments. I've seen that HSBC did question Mrs E about the £10,000 payment, but I'm not persuaded the conversation went far enough.

But, this in and of itself, isn't enough for me to say that HSBC should refund Mrs E the money she lost, I also need to be persuaded that sufficient intervention would have made a difference and prevented the payments from being made. Of course, I can't know for sure what would have happened had HSBC probed Mrs E further about these payments. So, I have to base my findings on the balance of probabilities – that is, what I think is more likely than not to have happened, taking into account what I know. Having thought carefully about this, sadly I don't think any further intervention at this point is more likely than not to have made a difference and stopped Mrs E from making the payments. I'll explain why.

I'm persuaded Mrs E would have been able to give plausible answers to any questions that HSBC could reasonably have been expected to ask. I think she would have been able to convincingly explain, that the payments were for her partner and that they'd been together for a number of years. Alongside this, given the level of detail the fraudsters had provided to Mrs E about the project they were supposedly working on/coupled with Mrs E's own personal experience of working with exports/internationally, I think she would have been able to provide credible answers to HSBC, had it probed her further about the nature of work B was undertaking. As well as this, by now Mrs E was aware of the real possibility of being challenged by her bank around the reasons for the payments she was making, and given her determination to make them, I think she would have been prepared for this, which would have made it all the more difficult for HSBC to uncover what was happening.

On balance, I'm persuaded the answers Mrs E would have given would more likely than not have satisfied HSBC that she wasn't at risk of financial harm. So I can't fairly or reasonably say that further intervention at this point would have made a difference.

Following these international payments, Mrs E goes on to make a payment for £10,850 (to a UK account), which was the fourth high value transaction, to new payees, within a month and she then starts to make payments to a cryptocurrency account.

HSBC has said that the first and third payments (for £500 and £6,400) to Mrs E's cryptocurrency account did flag on its fraud detection system and it spoke to Mrs E before allowing the payments to be progressed, but unfortunately those calls are no longer available and there are no contemporaneous notes to show that a robust conversation took place. I can't know for sure what was discussed, but looking at things in the round, on balance I think it was reasonable for HSBC to allow the payment for £500, and the payment that followed this, for £100 to be progressed. People can and do legitimately invest in cryptocurrency, and here Mrs E was making payments to a wallet that was in her name, and that she controlled.

But at the point where Mrs E attempts to send a payment to a crypto wallet for £6,400, I'm persuaded that her account activity had, by now, become so erratic, that I think HSBC ought to have had significant concerns that she was at risk of financial harm from fraud. And I'm not persuaded she would've been able to convince HSBC as to the legitimacy of the payments by this point had it sufficiently questioned her.

By now, it would have been evident to HSBC, that Mrs E had made multiple high value transactions to new payees and to international accounts and now, she was attempting a high value transaction for the purpose of purchasing cryptocurrency. Mrs E has told HSBC, during calls that it had with her relating to the international payments, that these payments were to help her partner who was stuck abroad, for a car for her stepdaughter, to pay the housekeeper's bills and for the purchase of investments in cryptocurrency – and, for the £10,850 payment to a UK account, I can see Mrs E referenced the payment as being for a caravan. While it is feasible for a customer to make a payment for any of these reasons, I consider it to be highly questionable, to the point of being improbable, that a customer would legitimately do all of these, over such a short period of time, for such large amounts, when it isn't the typical behaviour for that customer. It's also not lost on me, that HSBC would have been able to see large transactions coming into her account to facilitate the payments, including a cash deposit for thousands of pounds to seemingly fund an investment in crypto currency.

Given HSBC are the professionals here, I'd expect a bank to know better, than to allow further payments to be made. I'm minded, given the circumstances of the case, it's more likely than not Mrs E would have objected to HSBC's intervention and she would have tried to persuade it the payments were for genuine reasons. While Mrs E may have been able to speak confidently about the nature of work the fraudster had told her they were carrying out abroad and about the payments involving her step daughter and her carer, I'm not persuaded she'd have been as convincing when it came to discussing the payments to cryptocurrency wallets. I say that because she hadn't been provided with a cover story or a detailed reason as to why payments through crypto were necessary, so I'm minded to say she would have struggled to have plausibly answered questions HSBC could reasonably have asked about these payments.

Even if Mrs E hadn't accepted HSBC's intervention and not heeded the warnings, that I think it fairly and reasonably ought to have given, I think the nature of what was happening carried so many hallmarks of Mrs E being at such a significant risk of financial harm, that I think HSBC ought fairly and reasonably to have refused to make any further payments, in order to protect its customer from what I think was a clear and present risk of financial harm. With this in mind, I think HSBC is, at least in part, liable for the loss that Mrs E suffered when she made the payments for £6,400 and £10,500.

Should Mrs E bear some responsibility for her loss?

I have thought about whether Mrs E should bear some responsibility for the money she's lost by way of contributory negligence. The consideration of contributory negligence is an objective test but in considering what's fair and reasonable I've factored in Mrs E's vulnerability when considering the extent of any deduction for contributory negligence.

Mrs E has sent considerable sums of money based on requests from somebody she had never met in person, and only met just a few weeks before online. The reasons she was given by the fraudster for the requests included, lending some money for food and accommodation, needing money to save somebody's life from a gangster, through to under the desk payments to officials to cover a drug smuggling charge.

I understand that the nature of these scams, can often have a negative effect on a person's thought process and make them take steps that, in the cold light of day they might not otherwise take. But on balance, I'm not satisfied Mrs E, given the reasons for the payments given and the advice received from the police, airport security and her other bank ought to have believed this was a genuine situation and proceeded with the payments.

On that basis, I think Mrs E should share some responsibility for the loss and for a deduction

to be made on the losses for £6,400 and £10,500. Considering the individual circumstances of this case, I think that a fair and reasonable deduction would be less than we might typically order and I'm minded to say this should be 25%. Therefore, HSBC should refund 75% of these two payments.

Interest

I'm mindful that Mrs E has funded the payments to the fraudster through a number of different sources, including from various bank accounts, money transfers from credit cards, cash deposits into branches, loans from banks and loans from friends.

Given Mrs E's losses have come from various sources, it is my intention to take a pragmatic approach and say that an award of 8% interest is fair and reasonable in the circumstances.

In responding to my provisional decision, I'm happy to consider any further points or comments on this matter.

Summary

In summary, for the reasons explained, I'm minded to ask HSBC to refund Mrs E;

- *£32,850 (made up of the three payments for £12,000, £8,000 and £10,850 – being the payments that are caught under the CRM code).*

- *Pay 8% interest on this amount from the date it declined Mrs E's fraud claim until the date of settlement.*

- *£12,675 (being 75% of the final two payments Mrs E made to her crypto wallet).*

- *Pay 8% interest on this amount from the date of payments to the date of settlement.*

I have a great deal of sympathy with Mrs E being the victim of what was clearly a cruel scam that has had a significant impact on her. But it would only be fair for me to direct HSBC to refund the full amount of her loss if I thought it was wholly responsible for the failures that caused the losses. And for the reasons I've explained, I'm currently not persuaded that it would've been able to prevent Mrs E from losing all of the money she did.

I invited further evidence and comments from both parties.

HSBC responded. In summary, it said as a gesture of good will it was willing to agree to refund Mrs E in respect of the payments caught under the CRM code. But it didn't consider any refund was appropriate for the payments Mrs E had made to her cryptocurrency wallet.

It said that it had been told the cryptocurrency payments were towards Mrs E's investment portfolio and didn't accept there was a clear link between these payments and the earlier payments Mrs E had made. HSBC said that it didn't think giving a warning to Mrs E would have made a difference and even if it had stopped the cryptocurrency payments, it thought it was more likely than not that Mrs E would have found a way to make the payments by another method. Overall HSBC thought there were compelling reasons to illustrate why its intervention couldn't reasonably have made a difference.

HSBC added that, should it be required to refund Mrs E for the cryptocurrency payments, it considered that any reduction should be at least 50%. It said this because to the extent that it acted in error and could have made a difference, Mrs E's culpability should be at least

equal in respect of the cryptocurrency payments. This response from HSBC was shared with Mrs E.

Mrs E responded to my provisional decision and to HSBC's comments. In summary she said she was relieved that HSBC had agreed reimbursement of the payments which were covered under the CRM code. However, Mrs E said she was disappointed HSBC had taken the stance that it was not liable for the payments made to her cryptocurrency wallet. She added that at no point did HSBC invoke the Banking Protocol and/or ask sufficient questions, throughout her fraud. Mrs E added that HSBC was her largest creditor and that the amount of borrowing it had allowed her was unaffordable and irresponsible.

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 thank both parties for their responses to my provisional decision. Firstly, I note that Mrs E has said that she thinks HSBC were irresponsible in lending money to her that she says she couldn't afford. I would remind Mrs E of the comments I made in my provisional decision regarding this, if Mrs E wishes to complain about a financial institutions' lending decision, this is something she would have to take up with them in the first instance, to give them the opportunity to investigate. As HSBC hasn't had the opportunity to investigate these concerns, they don't form part of this decision.

HSBC has agreed to refund the payments Mrs E made that were caught by the CRM code and Mrs E has accepted this, so there isn't any need for me to comment on these particular payments any further in this final decision. The only remaining area of dispute seems to be around the payments Mrs E made to her cryptocurrency wallet, so I will focus on these below. I have thought about what HSBC has said about these payments since the provisional decision, but it doesn't persuade me to reach a different outcome.

Banks, such as HSBC, have clear obligations to protect their customers from the risk of financial harm and to prevent the furthering of financial crime. For the reasons explained in my provisional decision, based on what HSBC knew (and ought to have known had it enquired about the payments in the way that it should've done) at the time Mrs E was making payments to a cryptocurrency exchange, I think it should have had some serious concerns.

By this time, I'm persuaded, due to the nature of the payments Mrs E was making and the activity on her account, that HSBC ought reasonably to have identified that what was happening bore the hallmarks of a scam. Furthermore, if HSBC had questioned Mrs E about the earlier payments she'd made at this point, as I've explained I think it ought to have done, I think it could more specifically have considered the possibility that Mrs E was falling victim to a romance scam. Mrs E had multiple incoming credits, was making international payments to her 'partner' for work purposes and then making further payments for the purposes of supporting family members, followed by payments to cryptocurrency exchanges; all of which when considered together bear hallmarks of a romance scam.

I'm mindful HSBC has said the payments to cryptocurrency exchanges were for her 'investment portfolio', so there was no clear link to the previous payments Mrs E had made. But given the recent transaction history on the account, that HSBC was aware of, I don't think it was reasonable for HSBC to accept the purpose that Mrs E gave for the payments at face value. The lack of connection between the payments to the cryptocurrency exchanges and those proceeding them ought not to have reassured HSBC – instead it ought to have

been concerned about why Mrs R's account activity had so drastically changed compared to how it was normally used.

While HSBC doesn't agree, I think an appropriate intervention at the point Mrs E was making the payments to her cryptocurrency wallet would more likely than not have made a difference to the loss Mrs E incurred. And I say this having taken into account the previous interventions that another bank and third parties had made. With another bank being able to establish that Mrs E was falling victim to a scam and having taken steps to prevent money being lost at that point.

For the reasons explained in my provisional decision, I'm not persuaded Mrs E would have been able to plausibly answer further questions HSBC could reasonably have asked about these cryptocurrency payments, which I think would only have added to the concerns HSBC ought reasonably to have had at this time. As I have explained, with that being more likely than not to have been the case, HSBC had various options available to it. For example, it could have asked Mrs E to attend branch and invoke the banking protocol, it could have asked for evidence to satisfy itself that the payments carrying a risk of fraud (including those prior to the payments to the crypto exchanges) were genuine (which Mrs E wouldn't have been able to provide) and it could have declined to make the payments to the cryptocurrency exchanges altogether. HSBC didn't undertake any of these measures and in my view didn't fulfil its role in trying to protect Mrs E from a scam.

While HSBC believes Mrs E would likely have gone on to spend this money in any event this doesn't mean it had to allow her to do so. HSBC could've blocked the payments and put limitations on her account to prevent the loss to fraud. While these limitations couldn't have been put in place on a permanent basis, they could certainly have prevented the movement of these funds for a period of time.

It's relevant that the other bank involved in the scam was able to clearly identify Mrs E was at risk of a scam. Unlike HSBC it did put measures in place to prevent the scam but these didn't work. But this was much earlier in the scam journey and by the time Mrs E was making payments for the supposed purpose of purchasing cryptocurrency, the activity on her account was so much more concerning, with the reasons she was giving HSBC for the payments being made becoming more farfetched. This coupled with large amounts of funds coming into her account, from various sources, was indicative of a scam.

Therefore I'm persuaded there was a greater possibility for HSBC to have been able to identify and unravel the risk Mrs E was at and as such, a greater need for it to put in place more significant measures to protect her from harm. I'm persuaded HSBC ought fairly and reasonably to have prevented the payments to the crypto exchanges and put limitations on Mrs E's account to prevent further harm had it not been satisfied that following an intervention Mrs E wasn't going to spend the money anyway. HSBC allowed these payments to be processed and as a result is liable, at least to some extent, for the loss Mrs E suffered.

With all of this in mind and considering what is fair and reasonable in the circumstances of this case, I think HSBC is, at least in part, liable for the loss that Mrs E suffered when she made the payments for £6,400 and £10,500.

Finally, I've thought about HSBC's comments that liability should be shared equally to the extent that it is required to partially refund these payments. But, I remain of the view that, taking into account Mrs E's individual characteristics and vulnerability , I think that a fair and reasonable deduction to the redress is 25%.

Putting things right

I recognise the strength of feeling from both parties in this matter, but for the reasons explained I think it's fair and reasonable, in the circumstances of this case, to ask HSBC to refund Mrs E;

- *£32,850 (made up of the three payments for £12,000, £8,000 and £10,850 – being the payments that are caught under the CRM code).*

- *Pay 8% interest on this amount from the date it declined Mrs E's fraud claim until the date of settlement.*

- *£12,675 (being 75% of the final two payments Mrs E made to her crypto wallet).*

- *Pay 8% interest on this amount from the date of payments to the date of settlement*

My final decision

My final decision is that I uphold this complaint against HSBC UK Bank Plc in part.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs E to accept or reject my decision before 20 July 2023.

Stephen Wise
Ombudsman