Ombudsman Decision
CIFO Reference Number: 25-000482
Complainant: Mr W
Respondent: HSBC Bank Plc, Jersey branch ("HSBC")

The Complainant, who I shall refer to as Mr W, complains that HSBC should have intervened to prevent him from making, or to warn him against making, a large number of payments which were part of a relationship scam. The complaint has been brought on Mr W's behalf by a relative, so any reference to his submissions includes those made on his behalf.

Background

It is not in dispute that Mr W has fallen victim to a relationship scam and lost significant sums of money as a result. When the complaint was raised on his behalf, it was believed that the total losses arising from the scam were £68,495.92, US$42,732.63 and Aus$29,426.32. Those losses were the result of 53 payments made from four different HSBC accounts between January 2018 and April 2023.

When HSBC investigated the complaint, however, it identified 74 payments to the same recipient, beginning in December 2015. The US and Australian dollar payments were the same as those identified by Mr W, but there were additional payments made in sterling, bringing the total figure in that currency to £119,538.70. The bank's schedule of payments has been shared and is not disputed.

This is one of a number of scams of which Mr W has been a victim, some of which CIFO has already considered. His relative has provided evidence from health professionals which shows that Mr W has been diagnosed with frontal temporal lobe dementia. The initial diagnosis of some form of

dementia appears to have been made in 2023, but it is likely that the condition has been developing since around 2015. He says too that HSBC was, or should have been, aware of Mr W's vulnerabilities and should have intervened to prevent payments from being made from his accounts.

I understand that Mr W was contacted by someone (whom I'll refer to as "L") in an unsolicited telephone call. The details are not clear, but the payment schedule provided by HSBC suggests this must have been at some point before December 2015, when the first payment to L was made. Mr W has said that telephone contact continued for a long period, but it is not clear how long it was before the first payment was made.

Payments to a bank in the Philippines were made between December 2015 and April 2023. By this point, Mr W's family had become aware that he had been targeted by other fraudsters and were monitoring his finances more closely. They intervened and arranged for his telephone number to be changed, so there could be no more contact from L. This has prevented any further losses.

As far as they were able, Mr W's family reviewed his accounts and identified 53 payments to L. HSBC appears however to have identified a further 21 payments, going back a further two and a half years. They complained to HSBC on Mr W's behalf, saying that the bank should have taken steps to protect him from the scam. In saying that, they have said that the bank was or should have been aware of Mr W's vulnerabilities, given earlier scams where he had been targeted.

HSBC said it would contact the receiving bank, but that it did not expect (and does not expect) to make any recovery. It did not believe that it had any responsibility to make refunds, since the payments had been authorised by Mr W. The case was to CIFO in October 2025.

My preliminary assessment and the responses to it

I reviewed the evidence and arguments submitted on behalf of Mr W and HSBC. Having done so, I issued a preliminary assessment, in which I indicated that I was not minded to uphold Mr W's complaint or to require the bank to reimburse any of his losses. In summary:

- I accepted that Mr W had been tricked into making the payments.
- I accepted too what I had been told about Mr W's medical condition.
- My starting point was that a bank should usually follow its customer's instructions but should do so with reasonable care and skill.

- Mr W had authorised all the payments.
- The payments were out of character, at least initially.
- Whilst an after-the-event analysis indicated there were grounds for suspicion, I was not persuaded that HSBC should have intervened at the time the payments were made.
- I noted the submissions which had been made about the Contingent Reimbursement Model (or CRM) Code, adopted by the industry in the UK.
- I thought it unlikely that any of the funds could be recovered through the receiving bank.

Mr W's relative did not accept my initial findings and made further submissions. They said, again in summary:

- Even if the first payments were for relatively small sums, the tenth, which was for more than £10,000, should have triggered an alert.
- Previous decisions published by the UK Financial Ombudsman Service and case studies published by CIFO indicate that similar cases have been upheld in the past. It would be inconsistent with those cases to reach a different conclusion.
- The CRM Code says that banks should consider retrospectively whether the victim of an APP scam was vulnerable and, if so, reimburse them.
- There was no evidence that HSBC had warned Mr W of the risks of relationship or similar scams.

HSBC accepted my assessment. It also provided evidence of generic warnings which it said were shown at the relevant time.

As my initial assessment did not resolve Mr W's complaint, I have reviewed the case afresh before issuing this Final Decision.

Findings

I have considered all the available evidence and arguments to decide what is, in my opinion, fair and reasonable in the individual circumstances of this complaint. Where necessary or appropriate, I reach my conclusions on the balance of probabilities; that is, what I consider is most likely to have happened, in light of the evidence that is available and the wider surrounding circumstances.

In line with my statutory duty to disclose evidence, I have provided copies of the documents which I have relied upon in reaching my decision.

As I have said, I accept that Mr W was tricked into making the payments. He was led to believe that he was making them to help someone who was a genuine friend and in order to assist them financially. He says they told him they needed money for various reasons, including to fund medical and educational needs. Mr W says that the first contact was unsolicited and that there was never any face-to-face contact. That is consistent with relationship fraud, although I should note that in this case there is no supporting evidence – for example, by way of copies of any emails or text messages which might have been exchanged. Nevertheless, I agree that it is unlikely the money was used in the way L said it would be used.

I accept too that the medical evidence provided shows that it is unlikely that Mr W – even when the scam started – was able fully to assess the risks of making the payments. In addition, there has been a significant deterioration in his cognitive ability, both during the period when he was making the payments and since. I have taken that into account.

My starting point here is that a bank should generally follow its customer's instructions to make payments. The contractual position was set out in a relatively recent judgment of the UK Supreme Court (*Phillip v Barclays Bank Plc* [2023] UKSC 25) in the following terms:

"*It is a basic duty of a bank under its contract with a customer who has a current account in credit to make payments from the account in compliance with the customer's instructions. This duty is strict. Where the customer has authorised and instructed the bank to make a payment, the bank must carry out the instruction promptly. It is not for the bank to concern itself with the wisdom or risks of its customer's payment decisions*."

In carrying out its customers' instructions, however, a bank should act with reasonable care and skill. In some cases, that can mean it should go further than simply following instructions correctly; it should not, for example, ignore obvious indications that the customer does not understand what they are doing.

In addition, in deciding what I consider to be fair and reasonable in all the circumstances, I must have regard not only to relevant law, but also to what I consider to have been good industry practice at the time. And it may be good practice to intervene where, for example, the bank is aware of features of a transaction (or a series of transactions) which indicate that a customer may have been targeted by fraudsters.

I don't believe there is any dispute that Mr W authorised all the payments. That is, they were made on his instructions to the account in the Philippines which he told HSBC to pay. This is not a case where someone else managed to gain access to his account, or a case where the bank made payments other than in line with its customer's instructions. Mr W's argument is not that the payments were not authorised, but that the bank should have identified that they were unusual and should therefore have intervened.

To reach a fair and reasonable outcome, therefore, I have considered the following matters:

- Given what it actually knew about the payments, should HSBC have stopped them or raised with Mr W the possibility that he had been targeted by a fraudster?
- Was there anything about the nature of the payments which ought to have led the bank to ask further questions before completing them?
- If HSBC had acted differently before completing the transfer, would Mr W's losses have been avoided or reduced?

In some cases, a bank might know more about some aspects of a transaction than its customer does. For example, it might have received information about fraudulent activity on a receiving account. That was not the case here. HSBC knew no more about the payments than Mr W did. There was therefore no reason for the bank to stop or delay the payments (or any of them) because of anything it knew and which Mr W did not know.

I have therefore considered the second issue to which I referred above – namely, whether there was anything which HSBC did know about the payments which meant that it should, as a matter of good practice, have made further enquiries before completing them. HSBC has not suggested that it did make any further enquiries, and I have approached this case on the basis that it did not.

As I have said, I think the payments were out of character, in the sense that Mr W did not, at least at first, have any history of making payments to L or to the Philippines. HSBC's records show, however, that the initial payments were for relatively low amounts. There were also significant gaps between payments – sufficient for a customer to have raised the matter with the bank if, having made a payment, they thought something was wrong. For example, there was around three weeks between the first and second

payments and it was more than three months until the third payment was made.

The details of HSBC's fraud alert systems are, of course, confidential. But most such systems will be triggered by a combination of factors, including: the size of payment; whether the payment is to a new payee; the method of payment; and the device used to make the payment.

Most of the payments in this case were for relatively small sums – around £2,000 to £3,000. Only one, the tenth, was for more than £10,000; by the time that payment was made, it had been nearly eight months since the first payment. No issue had been raised about any of the earlier payments, and L was no longer a "new" payee.

Very often, scams like this one come to light because the fraudster demands ever increasing sums. That does not appear to have happened here, however, and in fact many of the later payments are for only a few hundred pounds.

Mr W's relative said in response to my preliminary assessment that, even if the initial payments from the account were relatively small, the tenth was for more than £13,000. At the very least, he said, the bank should be held accountable for that, and subsequent, payments. I accept that in some cases there may be good reasons for saying that an unusually large payment, even to an existing payee, may be grounds for suspicion. Here, however, I believe that the time which had already passed is a relevant factor, as is the number of previous payments to L. Mr W had had some eight months in which to reflect on the payments he had made but had not raised any concerns or, it would seem, had any reason to think that he was being scammed.

I acknowledged in my preliminary assessment that an after-the-event analysis of the payments gives grounds for suspicion and further investigation – not least because of the cumulative total paid from Mr W's accounts. However, that type of analysis in my view goes further than I would usually expect of a bank making checks to ensure that individual payments have been properly authorised and have not been induced by fraud. It also goes beyond what I would expect a bank to do as a matter of good practice.

I discussed in my preliminary assessment the CRM Code, which has been adopted by the industry in the UK. Whilst it has no direct application in Jersey and only applies to payments between UK banks from May 2019, I have taken it into account, as a further indication of what represents good

practice. In this case, some of the payments were made before the introduction of the Code, and all were made to an overseas bank. So, even if the payments had been made from a UK bank, the Code would have no direct application.

The basis of the CRM Code is that a customer who has been the victim of a scam of this type should be reimbursed, subject to certain exceptions. That is the opposite of the strict legal starting point, which is that a bank should follow valid instructions from its customers.

The exceptions include where the customer ignored effective warnings provided by the bank and where they have received a negative confirmation of payee. It is unlikely there would have been any confirmation of payee in this case, although the payments were of course made to the expected recipient in any event.

The information which HSBC has provided about warnings indicate that, until 2021, customers were advised to check that any payment request was genuine and that customers should check the details carefully. From 2021 the standard warning asked whether a customer had received an unexpected request to make a payment. It also referred to requests for payment from companies to which a customer might pay a bill, the bank or the police. It said too that the bank would never ask a customer to transfer money to a "safe" account. There was no specific reference to relationship fraud. I do not therefore believe that Mr W can fairly be said to have ignored effective warnings.

A further exception applies where the customer made the payment "… *without a reasonable basis for believing that … the payment was for genuine goods or services; and/or the person or business with whom they transacted was legitimate.*"

There were no goods or services involved here. In my view, the payments made were more in the nature of gifts, rather than being transactional. That might of course help to explain why Mr W did not query them at the time; since he was not expecting anything in return, he had no reason to do so.

In the circumstances, I do not believe that I can fairly say that HSBC should have intervened here, either to stop or to query the payments.

In response to my preliminary assessment, however, Mr W's relative has said that the CRM Code requires reimbursement where the customer is identified as having been vulnerable, even where any vulnerability was not apparent to the bank when any payments were made.

I have accepted the evidence of Mr W's medical condition and that it would have been deteriorating over the period when the payments were made. I agree that it is likely it would have made him vulnerable to scams of this sort. I have however seen nothing to show that HSBC was made aware of Mr W's medical condition at the time the payments were made.

I have therefore considered carefully whether – and having in mind the CRM Code – HSBC should have carried out a retrospective assessment of Mr W's vulnerability. That is, if the bank later found out that Mr W had been vulnerable, should it reimburse him, even though it did not know that at the time? I do not believe I can fairly say it should have done. As I have indicated, the CRM Code provides an indication of good industry practice. But in Jersey it does no more than that. And I must have in mind that, even if this complaint had been about a UK bank, the Code would have had no application, since all the payments were made to an overseas account.

Given my finding that HSBC was under no duty to intervene in the payments, I do not need to reach any conclusion about what might have happened if it had contacted Mr W to discuss them directly. In my preliminary assessment, I said that it was by no means certain that any intervention on the part of HSBC would have prompted him to stop making them.

In response, Mr W's relative has pointed out that, once the family intervened, he did stop making payments, even though he has had further contact from scammers. In my view, there is some force in the argument that this shows that Mr W would have been receptive to intervention by the bank, although it is impossible to know with any certainty what would have happened. Many victims of relationship fraud are comfortable with the payments they have made and do not heed warnings. But, as I say, that is not an issue on which I need to reach a conclusion, given my findings about the bank's obligations.

Where a customer says that they have been a victim of fraud, we would expect the bank to seek to recover funds. Given the time that passed between the payments and the bank being told that Mr W had been scammed, I think the bank's assessment that any recall request is likely to be unsuccessful is right. That is, the money has been lost, but I do not believe I can fairly say that the bank, rather than Mr W, should bear that loss.

Final Decision

For these reasons, my final decision is I do not uphold this complaint.

Mike Ingram
Ombudsman

23 February 2026