DRN-5490345

The complaint

Mr M, who is represented, complains that HSBC UK Bank Plc didn't reimburse him money he lost after he was a victim of fraud.

What happened

As the circumstances of this complaint are well-known to both parties, I have summarised them briefly below.

In June 2023, Mr M was looking for employment when he came across an opportunity online being advertised by a business I'll refer to as B. He completed an enquiry form and was contacted by a representative of B via a messaging app. Unfortunately, unbeknown to Mr M at the time, he was in fact talking with a criminal, intent on defrauded him.

As part of his purported employment, Mr M was told he would have to set up an e-commerce shop and buy products online for a percentage of their value. And once each product was sold from his e-commerce shop, he would receive a payment via an online account.

Mr M accepted the position and began making payments from his HSBC account to a cryptocurrency provider as instructed. He then forwarded this on to the wallet address provided by a representative of B.

Mr M could see via access to his online portal that his e-commerce business was doing well. But when he missed the deadline for one of his tasks, he was contacted by a representative of B and told he'd need to pay a substantial fine or risk having his account and online shop blocked.

Mr M eventually agreed to pay the fine, which he did through crypto purchases and bank-to-bank transfers from his HSBC account. But once this was paid, and he attempted to withdraw the earnings displayed in his online portal, he was then confronted with further fees.

When Mr M was unsuccessful in withdrawing the funds, he realised he was the victim of fraud and reported the matted to HSBC. For ease of reference, the following payments were made to the fraudster:

Payment date and type	**Amount**
30 June 2023 – card payment to crypto	£794.34
3 July 2023 – card payment to crypto	£2,857.82
5 July 2023 – card payment to crypto	£15,794.05
6 July 2023 – bank to bank transfer to a third-party account	£8,000

6 July 2023 – card payment to crypto	£100
7 July 2023 – Card payment to crypto	£7,891.41
18 July 2023 – bank to bank transfer to a third-party account	£7,750

HSBC looked into Mr M's claim but didn't offer a reimbursement of the funds lost. It considered the two bank-to-bank transfers under the provisions of the Contingent Reimbursement Model (the CRM Code) but concluded that it held sufficient evidence to decline Mr M's claim under the Code's exceptions to reimbursement.

It also considered the remaining card payments but found Mr M liable as he'd paid accounts held in his own name.

Mr M remained unhappy regarding HSBC's decision not to reimburse him, so he referred the matter to our service for an independent review. An Investigator considered the evidence provided but concluded HSBC's decision was fair in not reimbursing Mr M his loss.

Mr M, via his representative, disagreed. So the matter has now been passed to me to decide.

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.

Considerations

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.

Some of the transactions carried out as part of this fraud were authorised push payments (APP). So, when thinking about what is fair and reasonable in this case, I've considered whether HSBC should have reimbursed Mr M under the provisions of the CRM Code and whether it ought to have done more to protect him from the possibility of financial harm from fraud.

I'm persuaded that Mr M has fallen victim to a fraud. But this isn't enough for him to receive a reimbursement of the money under the CRM Code.

Under the CRM Code, a bank may choose not to reimburse a customer if it can establish that:

- The customer made payments without having a reasonable basis for believing that: the payee was the person the Customer was expecting to pay; the payment was for genuine goods or services; and/or the person or business with whom they transacted was legitimate.

Did Mr M make the payment with a reasonable basis of belief?

Having considered the evidence carefully, I'm not persuaded Mr M did hold a reasonable

basis for believing this was a legitimate business.

None of the evidence relating to the job opportunity presented to Mr M by B is available for me to consider. What Mr M has provided in terms of background is:

- The business contacted him because of an online form he'd submitted – so he wasn't approached via unsolicited contact.
- The business was registered on Companies House.
- Research left him satisfied the business was genuine.

While Mr M was contacted as a result of an online form he'd submitted, I'd still have expected him to have carried out due diligence on the business and, if he was satisfied the business was legitimate, that the person contacting him was legitimately from that business.

Mr M's representative has pointed out that a business bearing the same name as the one Mr M was contacted by was registered on Companies House. But has provided no credible link between the business Mr M was in contact with and that business registered on Companies House—such as the provision of a registered business number, website or contact information.

Nor has Mr M's representative provided any substantive evidence of research carried out on the business by Mr M, other than the results page of an online search engine: which bears no meaningful data.

What is more difficult here is that I am unable to analyse the original agreement between Mr M and B. There is no evidence available to demonstrate what Mr M's role was, how he would be compensated, and under what terms.

Nevertheless, Mr M's representative has submitted that it was his understanding the opportunity was one of employment, which poses some serious concerns as to why Mr M was required to make any payments to his employer in the first place; this goes against the typical employee-employer relationship where an employer is expected to make payments to its employee for work completed, and not the other way around.

Furthermore, at the point in which Mr M began to make payments covered by the CRM Code, on 6 and 8 July 2023, Mr M's representative has submitted that his online account displayed earnings of $50,000. These were earnings that had been made on his initial payments of circa £3,500. Mr M ought to have been alerted to these unrealistic earnings over such a short period of time: amounting to less than a week.

I do take on board Mr M's representative's submissions that he was presented with a professional online platform, provided a convincing and professional service by B and was given small, likely enticing, payments from B to his crypto wallet. But I don't find that these were enough to counter the lack of due diligence and suspicious claims I've highlighted above.

Overall, I'm persuaded that HSBC were fair when relying on the above exception to reimbursement under the provisions of the CRM Code.

Should HSBC have done more to protect Mr M from fraud?

There are two separate, but intertwined, considerations when thinking about whether HSBC ought to have done more here to protect Mr M from fraud:

- For CRM caught payments – HSBC's requirement to identify payments that are an

APP scam risk and to deliver effective warnings.
- For payments not caught by the CRM Code – whether HSBC ought reasonable to have identified payments that were out of character and/or unusual for the account, and intervened in those payments for the purpose of preventing financial harm from fraud.

Considering the above, I agree with the Investigator's assessment that HSBC ought to have intervened in the payments made. The Investigator has deemed the second payment, made on 3 July 2023, as an appropriate point at which HSBC ought to have contacted Mr M and probed the purpose of the payment further. I don't agree, as from looking at Mr M's bank statements, he had regularly made card payments for similar or higher values prior.

However, at the point Mr M made the third transaction subject to this dispute, on 5 July 2024, I do find that this was significantly out of character in terms of value. It also held a higher risk; in that it was being made to a business known for predominantly providing cryptocurrency. It was well-known to financial businesses at the time that crypto was being used by fraudsters to extract funds from victims of fraud in many cases.

Due to the amount being paid, and the additional risk associated with that payment, there was enough going on that ought to have reasonably alerted HSBC to a heightened risk of financial harm to Mr M. And I find that risk was significant enough that HSBC ought to have contacted Mr M and probed the reasons for that payment further.

Would any intervention have prevented Mr M from making further payments?

When considering both payments that are covered by the CRM Code, and those that are not, HSBC can only reasonably be expected to reimburse Mr M his loss where that intervention likely would have likely resulted in a prevention of his loss.

I can't know for sure what would have happened had HSBC intervened at the point I have said it ought to and delivered an effective warning. But I can deduce from events that occurred, and the evidence available, what is likely to have happened.

HSBC did intervene in a later transaction Mr M carried out in relation to the fraud. That intervention took place after Mr M attempted to make the fourth payment in the list above. During this call, a representative of HSBC attempted to ascertain why Mr M was making the payment. I have noted that throughout the call Mr M was overtly frustrated with the bank asking questions regarding the payment. He challenged the need for the representative to know why he was making the payment and was generally vague in his responses. But when Mr M did respond he wasn't, in my view, being entirely honest with HSBC.

In the call, Mr M responded to questions about the purpose of the payment stating that it was for the purchase of goods. When probed further, Mr M disclosed to the bank that it was a payment to a business he'd been affiliated with for circa a year. He also told the representative that he'd paid the account before, without issue, from an account held with another provider.

While I accept that the purpose of the payment could loosely be interpreted as accurate, Mr M hadn't been affiliated with the business for a year, and he'd not made payment to the account before. Mr M's representative has argued that Mr M had been in communication with B for a year prior to the call he had with HSBC, but that conflicts with the submissions it has made to this service previously—in that Mr M discovered the job opportunity in June 2023. It has also provided no evidence in support of this differing testimony. I must therefore conclude that its earlier submission is the more accurate of the two.

Taking the above into account, I find it likely that had HSBC intervened in the payment the previous day, it's likely that Mr M would have responded in a similar way. I have taken into account that the payment I have said HSBC ought to have intervened in was a card payment to a crypto platform, and not a bank-to-bank transfer to a business account. But that isn't enough to dissuade me that Mr M likely would have answered questions posed inaccurately. He hadn't been coached by the fraudster as to how to respond, but instead elected to mask the true reasons for the payment himself—and this would have thwarted HSBC's ability to protect him by delivering a warning relevant to his circumstances.

Job scams weren't as prevalent at the time Mr M made the transactions subject to this dispute, but investment scams involving cryptocurrency were. As Mr M likely wouldn't have revealed the true reasons behind why he was making the payments, or at the very least been vague enough to mask their true purpose, I find it reasonable that HSBC ought to have delivered an effective warning in line with the CRM Code regarding investment scams involving crypto payments. But this wouldn't have resonated with Mr M, as he wasn't falling victim to this type of fraud.

Overall, I'm satisfied that had HSBC intervened when Mr M made the third payment in the list above, it would have been unsuccessful in preventing Mr M from continuing to make payments to the fraudster. And had it delivered an effective warning regarding crypto investment scams, as I think it ought to have, this also would have been unlikely to prevent the fraud.

It therefore follows that it's unreasonable to hold HSBC liable for Mr M's losses.

Recovery of funds

Mr M, via his representative, hasn't disputed that HSBC ought to have done more to recover his losses, and this hasn't been a point of contention following our Investigator's view. But for completeness, and in summary, I have made the following observations:

- A significant time had passed between Mr M making the payments and reporting the matter to HSBC. It is common for fraudsters to quickly move funds from the beneficiary account where they are sent to circumvent money laundering prevention measures. It's therefore unlikely that HSBC would have been successful in recovering Mr M's losses.
- HSBC would have had no realistic prospect of success in raising chargeback claims to the crypto platforms where Mr M had made card payments to. The service those crypto platforms provide was given—in that it had converted the funds to digital currency for Mr M to move on. I therefore fund it reasonable that HSBC made no attempt to raise a dispute with those merchants.

In concluding

I know my findings will come as a disappointment to Mr M, and I am sorry he has been a victim of fraud. But I can only hold HSBC liable for his loss if it is unable to demonstrate an exception to reimbursement under the provisions of the CRM Code or where it ought to have done more to prevent him from continuing to make such payments. And in this case, I am unable to make such findings.

My final decision

For the reasons I have given above, I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr M to accept or

reject my decision before 26 June 2025.

Stephen Westlake
Ombudsman