DRN-6185933

The complaint

Mr J complains that HSBC UK Bank Plc ('HSBC') registered a Cifas marker against him, without due cause.

What happened

The circumstances of this complaint are well known to both parties, so I will not go into every detail of what happened here. But, in summary, In 2020 Mr J received a payment of £10,000 into his HSBC account, which was sent on to other accounts held in Mr J's name with other financial firms. HSBC later received notification that this had been sent to Mr J's account as a result of a scam. It asked Mr J about the funds, and he said he was not expecting the funds and did not authorise the ongoing payments from his account. HSBC asked for evidence from his other accounts, but this was not provided. It decided to close his account and refer him to Cifas for misuse of facility.

Mr J complained to HSBC, but it declined to uphold his complaint on the grounds that it did not think there had been any error on its part in closing his account and it had followed its obligations to report factual information to Cifas.

Mr J escalated his concerns to our service, where one of our investigators looked into what had happened. They did not recommend that Mr J's complaint should be upheld, on the basis that they thought HSBC had acted fairly and reasonably in referring Mr J to Cifas and closing his account. Mr J remained dissatisfied, and as no agreement could be reached the case has 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.

HSBC, as Cifas members, are obligated to share the details of customers who it has reasonable grounds to believe have been involved in the commission, or attempt to commit, fraud or financial crime. There must be *'clear, relevant and rigorous'* evidence in support of any fraud submissions made by members to Cifas about their customers. The type of Cifas marker loaded against Mr J was for 'misuse of facility'. This relates to a customer's account being used to receive and send on fraudulent funds.

Cifas do accept that there are some circumstances where an individual may be duped into becoming what is known as a 'money-mule', and so its guidance does require members to speak to their customers to determine whether they were witting or not. It further requires members to have enough evidence to show that the consumer was aware that they payment they were receiving was, or might be, from an illegitimate source – though they do not need to know the exact provenance of such funds.

So, the relevant findings for me to make are whether I believe there is sufficient evidence to conclude than on balance, firstly, that the money sent to Mr J was as a result of a fraud; and secondly that Mr J was aware that the funds he received were or might be from an

illegitimate source.

On the first point, it appears that it is common ground that Mr J did not have any entitlement to the funds that he received in his HSBC account. HSBC have provided evidence of the fraud report it received from the sending bank that shows that the funds were sent as a result of a scam, and Mr J on his part says that he was not expecting the payment into his account and was not responsible for sending the money onto other accounts.

So, I need to consider whether I think Mr J was involved in the receipt and transfer on of these funds, or whether he did not do this, or was unwitting in doing so. Mr J has explained that earlier in 2020 his phone was stolen, and it was unlocked. He said that he thinks that this may have allowed someone to access his HSBC mobile banking to complete the transactions. He said that his HSBC was not his main account at the time, preferring to use an account held with another firm, and so he had not been closely monitoring his HSBC account during this period.

I do not think that Mr J's explanation is most likely what happened here, I'll explain why.

- I have not seen any evidence in support of Mr J's position that his mobile phone was stolen earlier in 2020. But, even if a mobile phone is stolen, and it happens to be unlocked, there are additional layers of security information which are required to get into the HSBC app in order to transact on it. Whilst Mr J's phone being stolen would explain how use of his usual mobile device could be conducted without his consent, it does not explain how any of the additional layers of security were breached in this case. His explanation that banking apps may have been open when it was stolen does not seem to be a likely point of compromise, as access to his HSBC app would have required further biometric or passcode verification to keep it open – and an unknown third party could not have completed this. I would also have expected Mr J to contact HSBC without undue delay if he had his unlocked mobile stolen whilst he was accessing his banking app, which they have been able to demonstrate did not happen. So, I have not seen any plausible explanation as to how an unknown third party could have accessed his HSBC app in order to receive and send on the payments.

- I've considered whether someone else, without his phone, could have completed this transactions. This is because due to the passage of time, HSBC have been unable to provide me with the technical evidence to show that the transactions took place on Mr J's usual device. However, setting up the HSBC app on a new device and logging into Mr J's account would require additional security information and steps to completing them on his stolen device, and so for the same reasons, I cannot see how this could have been conducted by an unknown third party.

- Mr J was asked to provide his bank statements from an account held with another firm by both HSBC and our service. When he was unable to provide them, we gained copies of these statements ourselves. They show that the fraudulent funds were moved into this account in Mr J's name, and onto another account in the same day. This would mean that for this to have been done by someone unknown to Mr J, they also would have had to somehow breach the security of another account held with another firm. This does not seem most likely – as I have seen no plausible explanation as to how this unknown third party could have accessed the security information or otherwise breached the security of this second account, either.

- It would also seem highly unusual that an unknown third party, with access to Mr J's accounts simply waited some months in order to use his accounts, and then only to do so for money laundering purposes. Firstly, because this would risk losing access

to the accounts if Mr J had worked out that his accounts could be compromised. And secondly, because there were available funds on the account held with another financial firm, which they could have taken to add to their profits. This was left in the account.

- Mr J said that his main account was one held with another firm – but his wages came into his HSBC account, and payments labelled as rent (amongst others) left it. This demonstrates that it was an account of some importance, which makes me question why he said he was not monitoring it at the time. Indeed, there were payments in and out of the account in the days before and after the fraudulent funds entered his account. So, it seems more likely than not that this was an important account he would have kept an eye on. And in doing so, one would assume that he would have noticed the transactions. If Mr J had not known about the payments in and out of the account, I would have thought it would be likely that he would have reported them to HSBC before they asked him about them.

So, considering all of this, I think that the evidential threshold to apply a Cifas marker has been met in this case. And so it follows that HSBC acted fairly and reasonably in loading the marker, and I will not require it to do anything further.

My final decision

I do not uphold this complaint.

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

Katherine Jones
Ombudsman