DRN-4722755

The complaint

Mr L is unhappy HSBC UK Bank Plc ("HSBC"), won't refund the outstanding money he lost after falling victim to an authorised push payment ("APP") recovery scam whereby he sent money to an account held at HSBC.

What happened

The details and facts of this case are well-known to both parties, so I don't need to repeat them at length here.

In summary, Mr L fell victim to a recovery scam. Mr L was contacted by a company who advised that it could assist with the recovery of his funds from a company that Mr L had invested with that had gone into administration. Believing everything to be genuine, Mr L made a payment of £3,000 on 29 September 2022 from his bank account to an account held at HSBC. Mr L was advised that his recovered funds would be released – and when they weren't, Mr L realised he had been the victim of a scam.

After the scam was revealed, Mr L complained to his bank and also raised concerns about HSBC, where the receiving bank account was held.

Mr L's bank and HSBC are signed up to the Lending Standards Board's voluntary Contingent Reimbursement Model (the "CRM Code").

The CRM Code was implemented to reduce the occurrence of APP scams. The CRM Code requires firms to reimburse customers who have been the victims of APP scams like this in all but a limited number of circumstances. It sets out what is expected of the 'Sending Firm' and it also sets out the obligations for the 'Receiving Firm' to prevent, detect and respond to the receipt of funds from APP scams in order to prevent accounts from being opened, or used, to launder the proceeds of APP scams.

Where there is a failing by either the Sending Firm or Receiving Firm, they may be required to reimburse the customer. And the customer may also be required to share some responsibility for the loss if it is determined that one of the exceptions to full reimbursement, as set out within the CRM Code, applies.

Mr L's bank didn't agree that it was liable to reimburse him for the funds he had sent.

And HSBC, in its capacity as the Receiving Firm, also didn't consider it was liable for any loss Mr L incurred. But it advised it did manage to recover some funds from the receiving account (£195.03) which were returned to Mr L in November 2022.

Mr L brought the complaint about both his bank and HSBC to our service.

Mr L's complaint about his bank, as the Sending Firm, was looked at under a separate complaint reference. In that case, our Investigator considered that both Mr L and his bank should share responsibility for the loss. To put things right they considered Mr L's bank should refund 50% of the outstanding loss. Both parties accepted the Investigator's opinion and Mr L's bank refunded 50% of Mr L's outstanding loss.

In this case, Mr L says HSBC, as the Receiving Firm, should also share some responsibility. Mr L wants it to refund him the remaining loss as he considers one of its accounts was opened and being used fraudulently.

HSBC in its final response letter to Mr L didn't agree that it was liable for any loss Mr L incurred. It said that the account had been opened correctly and had been operating normally prior to receiving the payments – and it had no concern about the account usage prior to the report of fraud. It advised that following the report made against the account, it blocked the account, and recovered the remaining funds from the account which it had returned to Mr L. It further advised it investigated the account and took the appropriate action. Overall it found no errors in its handling of the receiving account or in the payment that it received from Mr L.

One of our Investigators looked into things and didn't recommend that HSBC needed to do anything further. Overall, they were satisfied HSBC had met the standards required of it under the CRM Code and wasn't responsible for Mr L's losses as it couldn't reasonably have done more to prevent Mr L's loss. They were also satisfied it had responded appropriately to the notification of fraud.

Mr L disagreed and asked for an ombudsman to review his complaint.

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.

First, to clarify, this decision focuses solely on the actions of HSBC – as the Receiving Firm of the account where Mr L made payment to. Mr L's complaint about his bank – as the Sending Firm was looked at separately under a different complaint reference.

I would also like to add at this point that I'm aware that I've summarised this complaint and the responses briefly, in less detail than has been provided, and in my own words. No discourtesy is intended by this. Instead, I've focussed on what I think is the heart of the matter here – which is to determine whether HSBC should have done more to prevent Mr L's loss. If there's something I've not mentioned, it isn't because I've ignored it. I haven't. I'm satisfied I don't need to comment on every individual point or argument to be able to reach what I think is the right outcome. Our rules allow me to do this. This simply reflects the informal nature of our service as an alternative to the courts.

I'm sorry to disappoint Mr L but I'm not upholding his complaint about HSBC. I know he's been the victim of a cruel scam, but I don't believe HSBC has acted unfairly or unreasonably in its answering of the complaint. I'm satisfied HSBC has met its requirements under the CRM Code and therefore isn't liable for any of Mr L's remaining losses. I'll explain why.

Among other things, regulated firms receiving payments like HSBC, are required to conduct their 'business with due skill, care and diligence' (FCA Principle for Businesses 2) and to comply with legal and regulatory anti-money laundering and countering the financing of terrorism requirements.

Those requirements include maintaining proportionate and risk-sensitive policies and procedures to identify, assess and manage money laundering risk – for example through customer due diligence measures and the ongoing monitoring of the business relationship (including through the scrutiny of transactions undertaken throughout the course of the relationship).

And, more generally given the increase in sophisticated fraud and scams in recent years, as a matter of good industry practice at the time, I think firms should reasonably have had measures in place to detect suspicious transactions or activities that might indicate fraud or financial abuse (something also recognised by the Banking Standards Institute's October 2017 'Protecting Customers from Financial harm as a result of fraud or financial abuse – Code of Practice').

And I'm satisfied that this good practice requirement meant not just looking out for situations where a customer might be the victim of fraud, but also situations where the customer might be the perpetrator of fraud or a money mule.

Also relevant in this case, as mentioned earlier, is the CRM Code that HSBC has signed up to.

The relevant overarching considerations for Receiving Firms under the CRM Code sets out the following:

> *"CRM Code: Payment Journey – Receiving Firm*
>
> *SF2 Receiving Firms should take reasonable steps to prevent accounts from being used to launder the proceeds of APP scams. This should include procedures to prevent, detect and respond to the receipt of funds from APP scams. Where the receiving Firm identifies funds where there are concerns that they may be the proceeds of an APP scam, it should freeze the funds and respond in a timely manner.*
>
> *Prevention*
> *SF2(1) Firms must take reasonable steps to prevent accounts being opened for criminal purposes.*
>
> *Detection*
> *SF2(3) Firms must take reasonable steps to detect accounts which may be, or are being, used to receive APP scam funds.*
>
> *Response*
> *SF2(4) Following notification of concerns about an account or funds at a receiving Firm, the receiving Firm should: respond in accordance with the procedures set out in the Best Practice Standards.*
>
> *SF2(5) On identifying funds where there are concerns that they may be the proceeds of an APP scam, Firms must take reasonable steps to freeze the funds and, when appropriate, should repatriate them to the Customer's Firm. Where appropriate, this should be done in accordance with the procedures set out in the Best Practice Standards."*

In considering all of the above, and to determine if HSBC met the standards required of it under the CRM Code, I have looked at whether HSBC opened the receiving account correctly, whether there was anything in the way the account was being used that should have given HSBC any cause for concern and finally; once notified of fraud did it act appropriately and in a timely manner. And if I consider there were failings in relation to any of the above, I have to consider whether HSBC's acts or omissions fairly resulted in Mr L's loss.

I would like to point out to Mr L at this point, that while HSBC has provided our service with information about the receiving bank account – it has done so in confidence. This is to allow us to discharge our investigatory functions and HSBC has provided that which is necessary for the determination of this complaint. Due to data protection laws our service can't share any information about the beneficiary, the receiving bank account or any investigation and action HSBC subsequently took. However, I would like to assure Mr L, I have thoroughly reviewed and considered all the information provided before reaching my decision.

Prevention - The account opening process

To help decide whether or not a bank failed to prevent the loss of an APP victim when opening the beneficiary account, we would generally ask to see evidence that; it correctly followed its account opening procedures; carried out checks to verify the identity of the named account holder; and did its due diligence when opening the account.

I appreciate Mr L has said he doesn't think HSBC has followed correct procedures as an account was opened and was subsequently used fraudulently. But in the circumstances of this complaint, I'm satisfied that HSBC carried out checks to verify the identity and address of the named account holder and did its due diligence when opening the beneficiary account. There wasn't anything at the time that I think reasonably could've alerted HSBC that the account it was opening would later be used fraudulently. So I'm satisfied HSBC has taken reasonable steps to prevent the account being opened for criminal purposes and it didn't miss an opportunity to prevent Mr L's loss when opening the account.

Detection - Account activity

The primary duty of a bank is to follow their customer's instructions and make payments as directed in line with the mandate – which is usually set out in the terms and conditions of the account. The CRM Code sets out that Firms must take reasonable steps to detect accounts which may be, or are being, used to receive APP scam funds. This ties in with long standing regulatory and legal obligations Banks and Building Societies have to monitor their business relationships and to be alert to other risks - such as fraud, which would include giving consideration to unusual and out of character transactions.

I've looked at the account history for the beneficiary account and I can't say there was any account activity that I think would reasonably have stood out to HSBC as suspicious or significantly outside of what might be expected for an account of that type. I'm also satisfied there was no notification of fraud on the account prior to the payment Mr L made into the account and no other red flags where it could reasonably be argued that HSBC might have had sufficient grounds to suspect fraud and refuse execution of their customer's payment instructions.

For Mr L's benefit, HSBC wouldn't have known that the incoming credit to the account was as a result of fraud and that its account was being used fraudulently. Personal and business accounts often receive incoming credits, and in this case, I think it is reasonable to say that there was nothing to indicate to HSBC at the time Mr L made his payment that there was anything suspicious going on with the beneficiary account.

So, from what I've seen, I'm satisfied HSBC has demonstrated that it has taken reasonable steps to detect accounts which may be, or are being, used to receive APP scam funds. I also don't think HSBC ought reasonably to have had concerns where I would have expected it to have intervened, so I can't fairly say that it could have prevented Mr L's loss in this way either.

Response to the notification of fraud

The Best Practice Standards set out that a Receiving Firm must take appropriate action, in a speedy manner, upon notification of APP fraud and notify the Sending Firm if any funds remain for recovery. Here, once notified of the scam, I'm satisfied HSBC took the necessary actions required of it and did so in a timely manner. Unfortunately, the majority of the funds had already been moved on / withdrawn from the account. But HSBC were able to recover what funds remained and returned them to Mr L.

So, taking the above into consideration I'm satisfied, following notification of APP fraud, HSBC responded in accordance with the procedures set out in the Best Practice Standards. And I don't think I can fairly say HSBC didn't do enough to respond to the alleged APP fraud.

Summary

Overall, while Mr L was the unfortunate victim of a scam, I'm satisfied HSBC met the standards required of it under the CRM Code. I also don't think HSBC could've done anything more as the Receiving Firm to have prevented the loss of Mr L's money. And it responded appropriately once notified of the fraud.

So, it follows that I don't think they are liable to reimburse Mr L for his remaining loss under the CRM Code or otherwise.

My final decision

For the reasons given above, my final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr L to accept or reject my decision before 19 December 2024.

Matthew Horner
Ombudsman