DRN-3470911

The complaint

Miss S seeks to recover around £15,000 from HSBC UK Bank Plc, which was stolen from her bank account in 2019 as the result of an investment scam.

What happened

Miss S fell victim to a scam in mid-2019, perpetrated by a firm claiming to offer profits by trading cryptocurrency. This outfit, called Pro Capital Markets, convinced Miss S to install applications and software onto her computer that gave them remote access to the device.

Miss S allowed this on the basis that her trading account would be set up so that she could begin the investment venture. Later that month, Miss S made a series of payments to what she thought was her trading account. Including, one card payment using her HSBC account on 24 May 2019 for £399.11 (the other payments were made using accounts elsewhere).

Shortly after making these initial investments, Miss S became worried that she couldn't get back the money she'd paid in. She had made withdrawal requests, but Miss S was noticing that her contacts at Pro Capital Markets were making excuses about her ability to take money out of her account, along with dodging her emails and calls. Because of this, Miss S got in touch with HSBC on 13 June 2019 to ask the bank to help her. Miss S says she told HSBC over the phone that she was having difficulty with the £399.11 card payment.

It's not entirely clear how the bank reacted to this. Miss S says she raised the payment as being fraudulent – but HSBC disagrees. The bank says that, rather than claiming she'd fallen victim to a scam, Miss S wanted to dispute a payment to a genuine firm on the grounds of *goods not received*. In other words, Miss S didn't mention that she'd been the victim of fraud.

Either way, Miss S didn't get a resolution to her dispute from HSBC by 17 June 2019, when Pro Capital Markets got back in touch in response to her withdrawal requests. At this point, Miss S was told she could withdraw her available balance within her trading account – but she would need to follow certain instructions and set up an account with AAA Trade in order to facilitate this.

Miss S was under the impression that AAA Trade was part of Pro Capital Markets and so she permitted the scammers remote access to her computer so that she could receive her investment back. But in fact, the scammers were actually paying money *out* of Miss S's HSBC account, into their own account(s). The use of AAA trade was merely a guise to get Miss S to make card payments to AAA Trade as an intermediary, so that her money could then be stolen.

To execute these payments, Miss S unwittingly passed over certain passcodes that HSBC sent to her in text messages. She did so because she thought that this was necessary so her money would be returned to her account. When in truth, the scammers were manipulating Miss S to share this information so that her money could be stolen using the remote access and security credentials she had passed over to set up her trading account.

What's more, the scammers also took out lending in Miss S's name, consisting of an £11,000 loan with HSBC.

Miss S says she was unaware of all of this. She accepts that she revealed passcodes that were sent by HSBC – but she was unclear what these were actually for at the time. As she remembers it, Pro Capital Markets justified the number of passcodes by telling her that these were a result of a system problem at HSBC's end. She was assured that this was normal and that she was only giving over the passcodes in order to get her withdrawal.

Miss S became aware of what happened shortly after payments were made out of her account on 17 June 2019. Upon being told by HSBC that she had lost all of her savings and taken on a host of debt, Miss S complained that the bank ought to have done more to protect her. HSBC declined her refund request, on the basis that she had allowed certain access to her security details and HSBC online banking facility. Miss S was also told she needed to repay the HSBC loan.

Unhappy with this, Miss S brought her complaint to our service. One of our investigators thought that HSBC should've noticed there was something untoward taking place with Miss S's account and intervened when the fourth card payment was made on 17 June 2019. In her view, this transaction in the sequence of payments stood out as uncharacteristic compared to her usual spending patterns.

However, under the circumstances, our investigator wasn't convinced that the bank stepping in at this point would've made a difference to whether the subsequent payments went ahead. So, our investigator didn't ask HBSC to return any of the disputed transactions. HSBC agrees with this assessment.

Miss S does not agree. She argues that any intervention from HSBC would've revealed that she was being scammed and she could've prevented her loss. Even more so, because she thought money was coming back to her and she had absolutely no idea about the loan.

Because Miss S disagrees, the case has been escalated to me to decide.

Provisional decision

I issued my provisional decision on this case on 21 April 2022. I have copied the findings and redress sections of my provisional findings below:

> *"I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.*
>
> *Having done so, I'm minded to reach a different conclusion to that of our investigator. The primary reason for doing so is on the basis of information that was provided by HSBC following our investigator's assessment.*
>
> *information received since our investigator's assessment*
>
> *It's always been common ground between the parties that Miss S contacted the bank on 13 June 2019 to ask for help with a payment she'd made the previous month. I asked HSBC to provide further details about what exactly was raised by Miss S at this time.*
>
> *HSBC submitted that its unclear what discussion was had, as the call recording is no longer available. But notwithstanding the phone conversation, Miss S also emailed the bank's disputes team the same day with supporting information. It's the contents of these emails which I've placed emphasis on when reaching my provisional findings.*

Miss S forwarded an email chain that her and Pro Capital Markets had exchanged in May 2019, at the time of making payments to what she thought was her trading account. The messages clearly show that the agent(s) of this firm had told Miss S to provide a host of personal information to open her trading account. Including, her photo ID, proof of address and details of her HSBC bank card.

It's evident from the emails that Miss S provided this information. Also, one of the more recent emails from Pro Capital Markets specifically asked Miss S to download an application called AnyDesk. This software's purpose was to grant remote access to Miss S's computer, so that Pro Capital Markets could control the device remotely.

relevant considerations

HSBC will be aware that there are some situations where we believe that banks – taking into account relevant rules, codes and best practice – ought to have been on alert or notice that something wasn't right or should have looked at the wider circumstances surrounding a consumer's account. So, I've looked into what this means for this case and whether HSBC should have done more to prevent the payments made on 17 June 2019, in light of the information Miss S had made it aware of four days prior.

First of all, the email correspondence Miss S shared with HSBC clearly showed that she had paid money into a so-called trading account. While AnyDesk itself is a genuine outfit that is legitimately used across many industries, I cannot ignore that HSBC was presented with documentary evidence that a supposed investment venture was asking for remote access to a consumer's computer.

As a bank that often sees all types of fraud, I'm satisfied that the mention of remote access, in the context of an investment where money couldn't be withdrawn, ought to have made it apparent to HSBC that this had the hallmarks of an array of common and well-known scams. Without a doubt, it's very unlikely that a genuine investment scheme would ask a consumer to download an application that gave it the ability to control their computer remotely.

I accept that it may not have been immediately apparent to HSBC that Miss S wished to dispute the payment on the grounds of fraud, based on the phone call alone. On account of the evidence, it seems that Miss S didn't even realise at the time that something fraudulent was happening. Therefore, I've thought carefully about what HSBC ought fairly and reasonably to have done under these circumstances.

I've borne in mind that there's a balance to be struck between identifying payment disputes between legitimate merchants and consumers where there is no risk of fraud, and those where the merchants or beneficiaries themselves are operating a scam. I also consider that the systems and procedures HSBC puts in place to manage those competing demands are a matter for the bank.

Nevertheless, the relevant standards and regulations – plus good industry practice – indicate that a bank does have a duty to protect its customers against the risk of fraud and scams so far as reasonably possible. HSBC ultimately has to make decisions based on the information its given by customers. And I find its neither unfair nor unreasonable to expect a bank to double-check disputed transactions when presented with information that ought reasonably to trigger concerns of fraud, or other risks of financial harm.

After all, if a bank is put on notice that there are suspicions of illicit activity, as the financial professionals, it is up to bank staff to find out enough information about what's happened in order to make an informed decision – and do so as quickly as possible.

Besides, HSBC didn't need to know for certain whether Miss S was dealing with a fraudulent cryptocurrency trader or investing in a legitimate product; reasonable grounds for suspicion are enough to trigger a bank's obligations under the various regulations and good practice.

In addition to concerns about payments already made out of Miss S's account, the emails demonstrated that Pro Capital Markets had a whole host of personal information for Miss S. HSBC were therefore presented with a consumer that was at real risk of financial harm from, amongst other things, identify theft. So, once in receipt of this information, I'm minded to find that HSBC ought to have been alive to the threat of further misuse of Miss S's account.

To that end, I believe there were reasonable grounds for HSBC to pause further activity on Miss S's account while it asked her for accompanying information. HSBC is permitted to temporarily suspend account movements (including card transactions and applications for lending) to avoid precisely this sort of situation. I think it would have been proportionate for bank staff to have asked Miss S to provide further details such as to whom the money was being paid to and why she had permitted remote access to her computer.

Having a conversation with Miss S about how her relationship with Pro Capital Markets had come about would most probably have revealed real cause for concern. I'm satisfied Miss S would have divulged that she had been contacted after seeing an advertisement from a celebrity on social media. One that had promised profits on cryptocurrency trades and that guaranteed withdrawals. But, despite being promised she could take out what she had put in, she was being restricted from accessing her money. And, crucially, these payments were being made possible via remote access to her computer.

Overall, had HSBC carried out further enquiries/research I find it highly likely it would have quickly established that Miss S was in the process of being scammed. At which point, I see no reason why HSBC could not have cancelled Miss S's card or taken action to prevent the subsequent payments from leaving her account.

Indeed, HSBC has said it would have done exactly that had it been aware that Miss S had fallen victim to a scam. Consequently, I intend to direct HSBC to refund these disputed payments.

<u>the HSBC loan</u>

As I've explained, I'm persuaded that the payments made on 17 June 2019 should have been averted. But for HSBC failing to act on information that ought reasonably to alert a professional banker to suspicion of fraud, Miss S would not be in the situation she now finds herself in; that being, having the liability to pay back a loan taken out in her name.

So, on those grounds, I am minded to conclude that HSBC shouldn't have let the events unfold on the day in question. However, for completeness, there is another reason why I propose that Miss S should not be held responsible for the loan.

Section 83 of the Consumer Credit Act 1974 outlines that a debtor under a regulated consumer credit agreement shall not be liable to the creditor for any loss arising from the use of the credit facility by another person not acting, or to be treated as acting, as the debtor's agent. In simpler terms, Miss S can't legally be held liable for a debt that another person, not acting on her behalf, took out.

Taking the above into consideration, I must first conclude – on the balance of probabilities – whether the loan was applied for by Miss S or an agent acting on her behalf.

Based on the evidence available to me, I think it's more likely than not that Miss S didn't apply for the loan herself. I say so for these main reasons:

- *While the loan application held Miss S's correct personal details, we already know the scammers had this information, having convinced her that it was needed to set up her trading account.*
- *HSBC hasn't been able to supply any substantive evidence to show the application details, such as Miss S's inputted income, was verified. In fact, HSBC is unable to show any real details of what information was used to submit the loan request.*
- *So, in the absence of any further evidence, I'm not compelled to believe that any specific information was given about Miss S that wasn't easily accessible to the scammers.*
- *Miss S has given a consistent and persuasive version of events, in the sense that she was completely unaware of any activity relating to her being responsible for a credit application.*
- *Although there may have been passcodes sent by HSBC to permit the loan going ahead, Miss S has given what she saw as a plausible explanation for why she gave this to the scammers – she was under the impression that this would permit her to receive money back from her investment. Much the same as one might input their PIN when receiving a refund in store.*

Based on all of the evidence available to me, I think it's more likely than not an unauthorised individual applied for the loan in Miss S's name. This is coherent with Miss S's statement and HSBC hasn't provided persuasive evidence to make me believe otherwise.

It follows that I intend to decide that Miss S neither applied for, nor agreed to, the loan in question. Accordingly, HSBC should put Miss S back into the position she would have been in, had the loan not been granted.

<u>putting things right</u>

For the loan, I propose that HSBC should remove all data/entries relating to the loan from Miss S's credit file. It's my intention that HSBC should also write off any remaining loan amount and refund all payments Miss S has made towards it.

In terms of the card payments, I have to bear in mind that the majority of what Miss S lost was enabled by the loan. Part of the loss was made up of her savings – so she should get those back in full. But without the loan, I can see that the entire £15,000 or so that was paid out of her account by the scammers would not have been possible. Where I am minded to necessitate that HSBC write off this debt, Miss S should not be expected to have this portion of the payments returned.

That being the case, it's my judgment that Miss S should receive the full amount that left her account, less the proceeds of the loan amount. Also, I intend to require HSBC to add 8% simple interest (per year) to this sum to recognise the loss of the use of these funds. This should be calculated from 17 June 2019 to the date of settlement.

My provisional decision

For the reasons given, I'm currently minded to uphold this complaint and require HSBC UK Bank Plc:

- *Write off any outstanding amount the loan might have*
- *Refund any payments Miss S has made towards the loan to date*
- *Remove any data in relation to this loan from Miss S's credit file*
- *Reimburse all of the disputed transactions that occurred on 17 June 2019 from Miss S's HSBC account, less the loan amount of £11,000; and*
- *Add 8% simple interest per annum to that sum from the date of loss to the date of settlement (less any lawfully deductible tax)."*

Responses to my provisional decision

Miss S accepted my provisional findings. And, with the intention of settling the matter, HSBC also agreed to my provisional decision on the grounds of paying the recommended redress as a gesture of good will.

Now that both parties have responded, the case has been returned to me for review.

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.

Given that both HSBC and Miss S agree to my provisional findings, I see no reason to depart from my proposed decision. To that end, the way in which I was minded to recommend that HSBC put things right remains the same.

My final decision

For the reasons given above and before, my final decision is to uphold this complaint and require HSBC UK Bank Plc:

- Write off any outstanding amount the loan might have
- Refund any payments Miss S has made towards the loan to date
- Remove any data in relation to this loan from Miss S's credit file
- Reimburse all of the disputed transactions that occurred on 17 June 2019 from Miss S's HSBC account, less the loan amount of £11,000; and
- Add 8% simple interest per annum to that sum from the date of loss to the date of settlement (less any lawfully deductible tax).

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss S to accept or reject my decision before 8 June 2022.

Matthew Belcher
Ombudsman