DRN-3235235

The complaint

Mrs C complains that HSBC UK Bank Plc trading as first direct won't refund transactions she didn't authorise.

What happened

In November 2020, Mrs C received a call from someone claiming to be from Amazon. They said they'd accidentally taken a payment from her account. And they needed her to provide a code from her first direct secure key to refund it.

Mrs C says she regularly shops with Amazon, and the caller didn't ask for her other bank details. So she trusted it was legitimate and gave them the code as instructed. The caller said the first code didn't work, so she generated a new one. But she became suspicious as they kept telling her it wasn't working, and to not turn her computer off. She ended the call, turned off her computer, and phoned first direct to explain what had happened.

Mrs C says it took around twenty minutes to get through to first direct. It locked her account and told her she'd receive a call from the fraud department over the next few days. But this didn't happen. She then received a letter confirming payments of £6,549.32, £7,876.31 and £6,987.21 had been taken on the day of the call. These were all international payments made to the same recipient, preceded by an internal transfer from Mrs C's savings account.

When Mrs C tried to call back to dispute these transactions, she says she couldn't get through due to the wait times. And when she did, she found out the account was still locked. First direct apologised for the service, but held Mrs C liable for the payments.

Our investigator didn't think Mrs C had completed the necessary steps to authorise the payments. Nor did they think sharing the code meant she'd been grossly negligent – or intentionally put her account at risk. They upheld the complaint and recommended that first direct should refund the payments, with interest, and pay £100 for the poor service.

At first direct's request, this case has been escalated to me for a final decision. It's agreed to the £100 compensation – but considers it unfair to be held liable for the financial loss. It says this was caused by Mrs C's negligence.

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.

Having done so, I've decided to uphold this complaint. I'll explain why.

Did Mrs C authorise the payments?

In line with the Payment Services Regulations 2017 (PSRs), Mrs C isn't liable for payments she didn't authorise, unless she failed with intent or gross negligence to comply with the terms of the account or keep her personalised security details safe.

First direct's most recent response – that it holds Mrs C liable due to negligence – suggests it may now accept that the payments weren't authorised. I'm satisfied that's correct.

There's no dispute the payments were properly authenticated via Mrs C's online banking. But to be authorised, the PSRs also require her to have *consented* to the payments. They also set out how consent is given; it's not open to interpretation. It must be given in the form, and in accordance with the procedure, agreed between Mrs C and first direct.

Based on first direct's submissions, and the explanation set out by the investigator in their view (which hasn't been questioned or contradicted), I understand the following steps were required for Mrs C to have consented to these payments – including giving someone permission to carry out these steps on her behalf:

- Log into her online banking. To do this, I understand Mrs C – or someone acting on her behalf – would need to enter her username, a secure key code, and the answer to her memorable question.
- Enter the payment information for the intended beneficiary for each payment.
- For the *first* payment, as this was a new payment destination, I understand it also required for a secure key code to be generated and entered. But the next two payments wouldn't have required this additional step.

Mrs C admits she generated and shared a secure key code a couple of times. But she didn't do this to get a refund, not to allow the caller to *make* payments. And the complaint summary first direct sent us sets out that the caller seemed to have *"obtained Mrs C's online banking username and the answer to her memorable question to then allow them to log on to her Online Banking with the [secure key] code Mrs C provided".* There's no suggestion she knowingly disclosed her username and memorable question to give the caller access to her online banking. We know that scammers often have ways of obtaining these kind of details, including asking unsuspecting questions to trick the consumer to reveal this information.

I consider it clear that neither Mrs C, nor someone with her permission, completed all the steps required to have consented to the payments – meaning they're unauthorised.

Did Mrs C fail with intent?

As Mrs C shared the secure key codes, she failed to keep her security details safe. But I don't think she did so *intentionally.* She shared the codes to receive a refund, not realising it would compromise the safety of her account and allow the caller to make transactions. So I'm satisfied she didn't fail with intent.

Did Mrs C fail with gross negligence?

First direct says that, by sharing her secure key codes, Mrs C was negligent and should therefore be held liable. But I'm not persuaded that, in sharing the codes, Mrs C was *grossly* negligent. The standard for that is whether she was *significantly* careless; whether she acted so far below what a reasonable person would have done; or seriously disregarded an obvious risk.

In the circumstances, I can see what Mrs C didn't immediately realise it was a scam. The caller seemed more plausible as she often shopped with Amazon, and as they already knew some of her details. As Mrs C told first direct at the time, she didn't think it was fraud as the caller didn't ask for her banking details (e.g. her sort code and account number) – so she didn't think there was a risk they were *taking* money.

Mrs C reasonably identified the risk when the caller *repeatedly* told her the code wasn't working, and kept telling her not to turn off her computer. But I don't think that, in being convinced by the call to share the codes initially, her actions fell so far below what a reasonable person would have done. In the circumstances, whilst she failed to keep her security details safe, I don't think she failed with gross negligence.

I therefore consider first direct liable for these payments. The investigator also awarded £100 for the distress and inconvenience caused by the way the claim was handled. Neither side disputes that the service was poor at times, or that £100 is a fair reflection of the impact this had on Mrs C. So I agree with this level of compensation.

Putting things right

HSBC UK Bank Plc should refund Mrs C for these three unauthorised transactions, totalling £21,412.84. As these funds were transferred from her savings account, that account interest rate should be applied to this amount – from the date of payment to the date of settlement. HSBC should also pay Mrs C £100 compensation for her distress and inconvenience.

My final decision

For the reasons given above, I uphold this complaint and direct HSBC UK Bank Plc to put things right as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs C to accept or reject my decision before 8 September 2022.

Rachel Loughlin
Ombudsman