DRN-5313946

## The complaint

Ms S complains that Starling Bank Limited didn't do enough to protect her from the financial harm caused by a scam, or to help her recover the money once she'd reported the scam to it.

## What happened

The detailed background to this complaint is well known to both parties. So, I'll only provide a brief overview of some of the key events here.

Ms S joined an online dating site where she met someone I'll refer to as "the scammer". They communicated via WhatsApp, email, calls, and video calls, but never met in person. The scammer said he was divorced, he had one son, and had moved to the UK after the divorce. They exchanged information about their background and seemed to have a lot of the same interests. He sent photographs of himself and his son and claimed to run a family business which was registered overseas.

Ms S believed the scammer was genuine and that they were developing a relationship. After five weeks, her asked her to send him some money because he was working overseas and his bank account had been blocked. He then contacted her on his return to the UK stating he needed money to pay solicitor's fees.

Ms S sent funds to the scammer from Bank B until 26 May 2022 when she was warned by Bank B that she might be the victim of a scam. A few days later, she began to send funds from her Starling account, and in December 2022 she stated sending funds from an EMI account I'll refer to as "W". Variously, she sent funds via faster payment and debit card to cryptocurrency exchange companies and via money remittance services. Between 31 May 2022 to 15 December 2022, she made 187 payments from Starling to eight different beneficiaries totalling £198,187.76. And, from 16 December 2022 and 22 May 2023, she made twelve faster payments from W totalling $72,591.93.

Unfortunately, she realised she'd been scammed when she found a person on social media that had the same photographs that the scammer had sent to her. She complained to Starling, but it refused to refund any of the money she'd lost. It said that for several of the payments, she was warned: *'are you being told to make this payment? Anyone telling you what buttons to click or asking you to read the text on this screen out loud is a criminal. You must not make the payment if you are being told how to answer the questions or explain the payment. Read each question carefully and answer truthfully, otherwise you could lose all the money sent'.* Ms S confirmed she understood the warning, she was paying 'friends and family', the payment was for a gift, and she'd met the recipient.

She was then shown a further warning as follows: *'Fraudsters will tell you how to answer these questions to scam you. A genuine organisation will never do this. A bank or any other organisation will never tell you to move money to a new, 'safe' bank account. Fraudsters can make phone calls appear to come from a different number. Are you speaking with who you think you are'?*

Ms S wasn't satisfied and so she complained to this service with the assistance of a representative who said Starling should have intervened because the account had previously been used for day-to-day spending, the largest payment on the account was £4,000, and she'd never bought cryptocurrency or sent international payments. They said Starling should have asked Ms S probing questions and had it done so it would have identified that she'd met someone through a dating site who had asked her to make payments in cryptocurrency for solicitor's fees.

Starling said the faster payments weren't covered under the Contingent Reimbursement Model ("CRM") code because they were to accounts in her own name. It said the payments were approved as they weren't deemed unusual, and Ms S was given sufficient warnings for the payments which triggered enhanced intervention. It explained that she said she was sending money to a family member or friend as a gift and that she'd met the person face to face, so there were no fraud concerns.

Our investigator didn't think the complaint should be upheld. She didn't think payments one to six were concerning because they were relatively low value. But by the time Ms S made payment seven she was satisfied this represented a clear change in the operation of the account and she thought Starling should have contacted Ms S.

She noted Starling intervened before payments 91,160 and 162, and Ms S was asked a series of questions and given written warnings tailored to the purpose she chose. She thought Starling should have done more on these occasions, but she didn't think further questioning would have made any difference.

She explained that Bank B had carried out a security check in branch on 26 May 2022. While she was on a call with the Fraud Team, Ms S was warned that she was falling victim to a romance scam, and she agreed for the payment to be cancelled. But in subsequent messages she had with the scammer, Ms S told him what Bank B had said and he told her it wasn't a scam and she started to send payments from Starling and, later from W.

Our investigator also noted that Bank B had intervened in July 2022 and that during the calls, Ms S was dishonest about the circumstances of the payment, advising that she was investing in Bitcoin and that she'd been doing so since 2017. She also confirmed that no one had asked her to make the payments.

She commented that when Ms S encountered issues with Bank B, she just made payments from a different bank, using various money remittance providers and cryptocurrency exchanges, which showed she was determined to make the payments.

Our investigator concluded that Starling should have intervened sooner and that it didn't do enough when it did intervene. But, as Ms S had continued to make payments following relevant warnings from Bank B and she misled Starling about the purpose of the payments when asked to provide a payment purpose, she didn't think this would have made any difference.

Finally, our investigator explained there wasn't a reasonable prospect of a successful recovery because Ms S sent funds to accounts in her own name and moved the funds onwards from there, and there were no chargeback rights because she would've received a service from the cryptocurrency merchants, so she didn't think Starling had acted unfairly when it considered Ms S's chargeback claim.

Ms S has asked for her complaint to be reviewed by an Ombudsman. Her representative has argued that Starling should have asked Ms S more probing questions and scrutinised her responses which could have uncovered the scam because Ms S was honest during the call

with Bank B, she didn't have a cover story and she was unable to provide consistent answers about cryptocurrency investments.

They dispute she was under the spell of the scammer because she decided not to go ahead with the payment after the May call. And even though Bank B's intervention stopped her from going ahead with the payment, it didn't stop the scam because the agent didn't confirm that she'd actually been scammed.

**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 reached the same conclusion as our investigator. And for largely the same reasons. I'm sorry to hear that Ms S has been the victim of a cruel scam. I know she feels strongly about this complaint, and this will come as a disappointment to her, so I'll explain why.

I'm satisfied Ms S 'authorised' the payments for the purposes of the of the Payment Services Regulations 2017 ('the Regulations'), in force at the time. So, although she didn't intend the money to go to scammers, under the Regulations, and under the terms and conditions of her bank account, Ms S is presumed liable for the loss in the first instance.

There's no despite that this was a scam, but although Ms S didn't intend her money to go to scammers, she did authorise the disputed payments. Starling is expected to process payments and withdrawals that a customer authorises it to make, but where the customer has been the victim of a scam, it may sometimes be fair and reasonable for the bank to reimburse them even though they authorised the payment.

*Prevention*

I've thought about whether Starling could have done more to prevent the scam from occurring altogether. Buying cryptocurrency is a legitimate activity and from the evidence I've seen, the payments were made to genuine cryptocurrency exchange companies and remittance services. However, Starling ought to fairly and reasonably be alert to fraud and scams and these payments were part of a wider scam, so I need to consider whether it ought to have intervened to warn Ms S when she tried to make the payments. If there are unusual or suspicious payments on an account, I'd expect Starling to intervene with a view to protecting Ms S from financial harm due to fraud.

The first two payments were to a cryptocurrency exchange company, but Starling didn't need to intervene because the payments were very low value. And I agree with our investigator that it didn't need to intervene in the next four payments because they were relatively low value and Ms S was sending the funds to an online money transfer service. However, by the time Ms S made the seventh payment, the cumulative total for the day over three payments to the same payee had risen to £5,572.93 and this was significant for the account, so Starling should have intervened.

I've also thought about whether there were other occasions when Starling should have intervened and I've noted that on 22 July 2022 Ms S made three payments in one day totalling £9,352.82, on 3 August 2022 the cumulative total was £15,384.77, and on 10 September 2022 the total spend for the day rose to £22,763.96. On those dates, Ms S was sending funds of varying amounts to several different money transfer services, and the account had developed a pattern of spending which meant this wasn't unusual. However, I agree with our investigator that, considering the general operation of the account over the weeks and months that followed, it ought reasonably to have intervened again at some point.

However, I've considered what happened when Starling did intervene as well as what happened when Bank B intervened before the payments she was making from that account, and I don't think there was anything else Starling could have done to prevent the scam.

Ms S was required by Bank B to attend a branch on 26 May 2022 because of doubts about a payment she was attempting to make to a cryptocurrency exchange. During the call she had while she was at the branch, she explained she was sending funds to a gentleman overseas who she'd met four weeks prior because he needed to get into his UK bank accounts. She said he'd been working there for a week, and she planned to send a total of £16,000. The call handler told Ms S that she thought she was the victim of a romance scam and Ms S was happy for the payment to be cancelled, but she didn't believe she'd been scammed. In response to this the call handler arranged for the account to be blocked to prevent her from making any further scam payments.

Significantly, she started to make payments from Starling after she was told by Bank B that she was the victim of a romance scam, and the messages she sent to the scammer when she left the bank show she didn't believe what she'd been told and still trusted him.
I've also listened to the calls Ms S had with Bank B about a payment she was making to a cryptocurrency exchange on 15 July 2022 and its clear she misled the agent throughout. She was open about the fact she was buying cryptocurrency, but she said there was no third party or friend involved and that she wasn't being forced to make the payment. I'm satisfied that Bank B did ask probing questions – it asked which cryptocurrency she was buying, whether she been asked to download remote access software, whether she'd invested before, whether she was aware of the risks and whether she'd done any due diligence – and I don't think there was anything else it could have asked to either uncover the scam or to prompt Ms S to disclose any more information.

Its clear Ms S was frustrated at having to spend time on the phone to the bank and the subsequent messages to the scammer she even suggested sending funds via a third party who could then forward the funds to a cryptocurrency merchant to avoid further calls with the bank.

Starling has explained that it intervened before the payments Ms S made on 2 August 2022, 29 September 2022, and 30 September 2022. On those occasions she said she was sending gifts to friends and family, she'd met them face to face, she hadn't been asked to send money unexpectedly, and she hadn't been asked to make the payment due to some form of problem or emergency. She was then warned: '*Fraudsters will tell you how to answer these questions to scam you. A genuine organisation will never do this. A bank or any other organisation will never tell you to move money to a new, 'safe' bank account. Fraudsters can make phone calls appear to come from a different number. Are you speaking with who you think you are'?* Ms S confirmed she understood the warning and proceeded with the payments.

I'm satisfied Ms S's responses to the questions she was asked prevented Starling from identifying that she was the victim of a scam. I'm also satisfied that as she was sending around £2,000 to £2,500 via legitimate merchants, the warning was proportionate to the risk and relevant to the information Starling had available.

Ms S was also asked to provide a payment purpose when she made payments from W, but each time she gave an inaccurate response which likely prevented it from providing a relevant warning.

Based what happened during the various interventions, I don't think there was anything that Starling could have done to prevent Ms S's loss. Her representative has argued that she told

Bank B about the scammer, and she'd have provided the same information to Starling if it had asked her more probing questions and subjected her inconsistent responses to closer scrutiny. While I accept that she did disclose the existence of the scammer to Bank B, she later lied to Starling and W. By the time I think Starling ought to have intervened, she'd decided not to tell the bank about the involvement of the scammer and the messages she had with him around the time of the first payment from Starling show she was being coached.

Further, the fact Ms S made payments from Starling after being told by Bank B that she was being scammed shows she chose to believe what she was told by the scammer over what she'd been told by Bank B. And the fact she tried to think of alternative ways to send the funds when it became increasingly difficult in July 2022 shows she was determined to make the payments and that she maintained this attitude until May 2023.

So, while I agree with our investigator that Starling missed opportunities to intervene and that it should have asked more probing questions, I don't think it could have uncovered the scam and I don't think there was anything it could have said to Ms S in terms of warnings or scam education which would have prevented her from making the payments. So, I can't fairly ask it to do anything to resolve this complaint.

*Recovery*

I don't think there was a realistic prospect of a successful recovery because Ms S paid cryptocurrency accounts in her own name and moved the funds onwards from there.

Ms S's own testimony supports that she used cryptocurrency exchanges to facilitate some of the transfers. Its only possible to make a chargeback claim to the merchant that received the disputed payments. It's most likely that the cryptocurrency exchanges would have been able to evidence they'd done what was asked of them. That is, in exchange for Ms S's payments, they converted and sent an amount of cryptocurrency to the wallet address provided. So, any chargeback was destined fail, therefore I'm satisfied that Starling's decision not to raise a chargeback request against the cryptocurrency exchange companies or the money remittance services was fair.

The Contingent Reimbursement Model ("CRM") Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, in all but a limited number of circumstances. Starling has said the CRM code didn't apply to the faster payments because Ms S was sending funds to accounts in her own name, and I'm satisfied that's fair.

*Compensation*

The main cause for the upset was the scammer who persuaded Ms S to part with her funds. I haven't found any errors or delays to Starling's investigation, so I don't think she is entitled to any compensation.

Overall, I'm satisfied Starling took the correct steps prior to the funds being released – as well as the steps it took after being notified of the potential fraud. I'm sorry to hear Ms S has lost money and the effect this has had on her. But for the reasons I've explained, I don't think Starling is to blame for this and so I can't fairly tell it to do anything further to resolve this complaint.

**My final decision**

For the reasons I've outlined above, my final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms S to accept or reject my decision before 16 April 2025.

Carolyn Bonnell
**Ombudsman**