

The complaint

Mr F complains that Starling Bank Limited (Starling) won't refund the money he lost as a result of a safe account scam.

What happened

I issued my provisional decision on this complaint on 16 February 2024. I wanted to give both sides a chance to provide any further evidence and arguments before I issued my final decision. That provisional decision forms part of this final decision and is copied below.

What happened

Mr F interacted with a text message he received concerning a government Energy Bill Support Scheme, and in doing so shared his bank card details for his account with another bank (that I'll call H).

On 21 September 2022, Mr F was called on a private number supposedly by H. Unbeknown to Mr F, he was speaking to a fraudster. Mr F queried how he could be sure he was speaking to H, at which point the fraudster advised Mr F how to search H's online banking team's phone number and then called Mr F back from this number.

Mr F said the fraudster knew his address and told him there'd been unusual activity on his account with H. They asked if Mr F had recently applied for a government scheme or transacted in bitcoin. When Mr F recalled the text that he'd recently received, the fraudster explained this was how his account had been compromised. The fraudster instructed Mr F to move his funds to a 'secure account' or face losing his money.

Mr F firstly moved funds from his account with H to a third party payee (payee 1). The fraudster then asked if he had other accounts as they could be affected too. When Mr F confirmed he had a Starling account, the fraudster said someone was trying to take his balance, so he also had to secure the funds in his Starling account. Mr F proceeded to make 15 payments to a different payee (payee 2) from his Starling account. During these payments, the fraudster told him to move further funds from H to Starling in order to secure more money from H. These funds facilitated some of the payments he made from his Starling account to the fraudster.

Whilst Mr F was moving money from his Starling account, the fraudster asked Mr F for control of his computer for ease and pace. But Mr F has confirmed that to the best of his recollections, the scammer did not make any payments using remote access. Mr F attempted three more unsuccessful payments to a different payee (payee 3) from his Starling account. The first was declined and the next two (attempted the following day) were cancelled.

Mr F then moved on to a third account with another bank (that I'll call M), but the transaction was blocked by M. The fraudster told Mr F to wait an hour for everything to go back to normal and ended the call. Mr F described a sinking feeling as he started to think he'd been scammed. He then called H who confirmed his suspicions.

Mr F reported the scam to Starling using its chat service at 11:20 on 22 September 2022. Starling contacted the bank Mr F sent his funds to at 14:38 the same day, but it didn't get a response. Starling declined Mr F's claim on 10 November 2022 because it had sufficient fraud prevention measures in place, and Mr F didn't take reasonable steps to check the payments were genuine. But it did pay Mr F £75 compensation for the delays to assessing his claim.

Unhappy with Starling's response, Mr F referred his complaint to this service and our Investigator partially upheld it. They considered the Contingent Reimbursement Model (CRM) Code which Starling is a signatory of. The CRM Code requires firms to reimburse customers who have fallen victim to an authorised push payment (APP) scam (like Mr F), in all but a limited number of circumstances. Our investigator said Mr F ought to have had concerns about the payments he was making. So, under the CRM Code, he didn't have a reasonable basis for believing that the person with whom he transacted was legitimate. But they also said the warnings given by Starling weren't Effective Warnings, and it ought to have intervened and discussed the activity with Mr F by the third payment. So, they recommended that Starling put things right by:

- Refunding 50% of the loss resulting from payments 3-15
- Paying the applicable account interest rate from the date of loss to the date of settlement on the refund of the payments made using the funds that were already in Mr F's Starling account
- Paying 8% simple interest from the date of the loss to the date of settlement on the refund of the payments made using the funds deposited into the Starling account from Mr F's (H) current account.

Starling didn't accept our investigator's recommendations. It questioned why our Investigator hadn't assessed the payment review model (PRM) warnings it gave Mr F. It said these were specific to the scam Mr F fell victim to, and this should have been a major red flag to Mr F. Starling also said the values of the payments and references input by Mr F meant the payments wouldn't have alerted it to the possibility of a scam.

As no agreement could be reached, this case was passed to me for a decision to be issued.

What I've provisionally 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.

In doing so, I'm required to take into account relevant: law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to be good industry practice at the time.

Mr F acknowledges he carried out the transactions in dispute, albeit he was tricked into doing so. Under the relevant regulations, namely the Payment Services Regulations 2017 (PSR 2017), Mr F is responsible for transactions he has authorised.

However, as I've already set out Starling is a signatory of the CRM Code. The starting position under the CRM Code is that Starling ought to refund Mr F, unless it can establish an exception to reimbursement applies. Such exceptions to reimbursement include (as far as is relevant to this complaint) that Mr F:

- Ignored an Effective Warning by failing to take appropriate actions in response to

such an Effective Warning and/or

- *Made the payment without a reasonable basis for believing that the payee was the person the Customer was expecting to pay; the payment was for genuine goods or services; and/or the person or business with whom they transacted was legitimate.*

Starling is relying on both exceptions to reimbursement. In this case, I think that Starling can rely on one of those exceptions – that Mr F lacked a reasonable basis for believing that the person or business with whom he transacted was legitimate. I know this might be disappointing for Mr F, so I'll explain why I've reached this decision.

Mr F says it was the spoofed phone number which persuaded him of the caller's legitimacy, but our Investigator and Starling didn't agree that the number belonged to H. Evidence of the call log isn't available, so I've weighed up what most likely happened on the balance of probabilities.

I think the phone number used by the fraudster likely was spoofed to match H's online banking team as Mr F says. I say this because having looked into it, the number Mr F gave Starling was one digit different to H's online banking team's phone number. Mr F has maintained throughout his testimony to Starling and our Investigator that the phone number the fraudster used was spoofed to mimic H's online banking team's phone number. Given how specific Mr F was about the fraudster calling back on this phone number, after he challenged the private number, and how he described being talked through validating this number, I think it's unlikely he'd have been reassured if the number didn't actually belong to H in the way he said. It's also entirely possible Mr F mis-typed the phone number when he gave it to Starling, as there's a difference of only one digit. Mr F has since clarified to our Investigator what the phone number was, and it is indeed a complete match to H's online banking team. Therefore, unlike our Investigator, I'm persuaded the number likely was spoofed.

I appreciate how compelling a spoofed phone number would have likely been to Mr F, especially as he says he didn't know about spoofing before the scam. I can also see why he might have believed H had reason to contact him in the initial stages of the scam, given he'd compromised his card details for his account with H through a fraudulent text message prior to the phone call. But it remains unclear how this meant his Starling account was also compromised. I've seen nothing to suggest Mr F had compromised his Starling account information in the same text message. And there's been no explanation given as to why his funds weren't safe in his Starling account. It seems the fraudster only told Mr F that any bank details he held were compromised, with no further explanation and this was taken at face value.

I also think that as further payment requests were being made of Mr F, he ought to have become more concerned about the legitimacy of the phone call. Mr F first made two payments from his account with H to payee 1. From his Starling account, he sent further funds to payee 2 and payee 3. As Mr F was moving funds to his own 'secure account' I think he ought to have been concerned that he was sending his funds to various third parties' accounts at external banks. No plausible explanation was provided by the fraudster as to why the funds were not going to an account in Mr F's name, or why H would be instructing him to send his funds to another bank which was not linked to H or Starling. And Mr F has confirmed he didn't really question this at the time.

The fraudster also told Mr F to enter unusual payment references to the payments being made like deposit, sofa, carpet, boiler repair etc. Mr F says he was told what to enter and there was no explanation given as to why. He didn't question this as he thought he was speaking to a bank staff member. However it's unclear to me why a bank staff member

would instruct someone to enter unrelated references to payments being made. I think this ought to have stood out to Mr F as unusual at the time and he ought to have challenged this.

Despite Mr F suggesting he didn't ask questions because he thought he was speaking to a bank staff member, he told our Investigator that he was questioning the fraudster continuously, suggesting he did have concerns. For example, he asked the fraudster to confirm the balance in his ISA with H, but it said it couldn't do this due to data restrictions. I think most banks would be able to confirm the balance in a customer's own account held with that bank, so I don't find this to be a satisfactory response to Mr F's question. And I think the self-admitted repeated questions asked, show Mr F also wasn't entirely satisfied by the fraudster's story.

Furthermore, Mr F has described how the fraudster contacted him on WhatsApp from a mobile number. I think it's unusual for a bank to use this method of contact to discuss a customer's account. These messages are no longer available, nor can Mr F recall what was said in them. So, I've not seen evidence to lead me to believe that the correspondence was particularly professional or persuasive.

I also believe that the warnings Starling gave Mr F, contained some specific information which ought to have resonated with him at the time. The warnings started off by saying (screen A):

"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."

Whilst Mr F told Starling he was 'Buying items or property' through a 'Family member or friend', the warning did still contain information relevant to safe account scams such as coaching. The warning went on to say (screen B):

"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?"

Mr F says that whilst he did give the scammer remote access, to his knowledge he doesn't recall the fraudster making any payments at any point. So I'm satisfied it was Mr F who went through the payment journey and therefore was presented with the online warnings.

Mr F says he was coached through these warnings, and claims they appear on all payments from Starling. He says he was reading the warnings out to the fraudster and was being told what answers to give, as he was convinced that he was speaking to a bank staff member. But as he was under stress, it was all a blur.

However the very first part of the warning resonates entirely with what he was doing –
"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.”

I also understand Mr F felt rushed, and didn't have time to think, for fear he'd lose his money. However, the evidence shows the PRM warning began at 17:40:41 and he didn't get to the final screen until 17:42:49, with approximately 36 seconds on screen A. Whilst two minutes might not seem like a long time outside of this context, in a payment journey I think this was sufficient time for Mr F to have read the warnings being presented to him and I think they ought to have resonated with him.

It's for these reasons I find that Mr F lacked a reasonable basis for believing that the person or business with whom he transacted was legitimate, and therefore Starling has fairly established a valid exception to reimbursement applies under the CRM Code. As one exception to reimbursement applies, I don't need to consider whether further exceptions fairly apply, as this has no impact on Mr F's liability.

Did Starling meet the standards for firms under the CRM Code?

Starling also has standards it's expected to meet under the CRM Code. Failure to do so in relation to a particular payment, or series of payments, could mean it's responsible for partially reimbursing its customer.

The CRM Code requires a firm to provide an Effective Warning where it identifies an APP scam risk in a payment journey.

As I've set out above, Starling gave a warning for the first payment Mr F made, based on the answers he provided to the automated questions asked. Our Investigator said this warning was not an Effective Warning because it wasn't specific to the scam Mr F was falling victim to, and therefore Starling should be partially liable.

However, it's important to consider that as Mr F misled Starling about the true reason for the payment, this seriously impacted Starling's ability to provide Mr F with an Effective Warning. So it would not be fair to say it failed to meet the standards for firms on the basis the PRM warning was not an Effective Warning.

Where my decision again differs to our Investigator's is that I'm satisfied Starling wasn't required to present Mr F with a further warning for the next two payments as they were unremarkable in value, and it had already established the reason for the payments to this payee during the first payment. Overall, Starling has no liability for the first three payments as a valid exception to reimbursement applies, and it would not be fair or reasonable to say Starling failed to meet the standards for firms.

However, by the fourth payment I'm persuaded a heightened APP scam risk ought to have been apparent to Starling, and it should no longer have been satisfied by Mr F's responses to the initial PRM warning. I'm persuaded Starling, fairly and reasonably and taking into account what the CRM Code requires, ought to have done more than just provide Mr F with a written warning by the fourth payment. Under SF1(5) of the CRM Code, it says that "Where a firm has sufficient concern that a payment may be an APP scam, it should take appropriate action to delay the payment while it investigates." I think this applies to the fourth payment Mr F made such that Starling ought to have gone further than provide a written Effective Warning.

I say this because Mr F had now made four transactions to a new payee, in less than 10 minutes. The beneficiary bank the funds went to was also one which specialises in pre-paid cards; in my experience this is a payment method often favoured by fraudsters. And whilst

the values of these payments were fairly low, they were unusually similar in value, which can be consistent with certain scams. In my opinion, a clear pattern which was consistent with fraud formed here and Starling ought to have provided a proportionate response to the apparent risk presented.

Starling should have contacted Mr F to discuss the recent activity on his account, to ensure he wasn't being defrauded. Had it done so, I think Mr F likely would have been honest. Whilst Mr F was being coached through the online written warnings, and therefore may not have properly taken on board the written warnings being given, I don't think the outcome would have been the same had Starling verbally warned Mr F that he was being scammed. He wasn't given a sophisticated cover story, beyond how to answer the questions in the online written warning. And he thought he was moving his funds to keep them safe. Had Starling brought to life the common features of a safe account scam, such as number spoofing, and warned him that he was doing the very opposite of keeping his funds safe, I think this likely would have reinforced the concerns Mr F held at the time and he wouldn't have proceeded with the payments. Especially as it seems Mr F's belief was heavily reliant on the spoofed phone number, which Starling could have quite easily explained in more detail than the online written warning did. Therefore, had it not been for Starling's lack of intervention on the fourth payment, Mr F wouldn't have gone on to lose this money. So, Starling can fairly and reasonably be held liable for Mr F's loss from and including the fourth payment.

Recovery of funds

Finally I've considered whether Starling acted reasonably in its attempts to recover Mr F's funds. I'd have expected Starling to contact the beneficiary bank immediately (or within an hour) in line with the Best Practice Standards for recovery of funds. Whilst Starling failed to do this, evidence from the receiving bank shows Mr F's funds were utilised prior to him reporting the scam. So, any delay from Starling didn't impact the amount recoverable from the beneficiary bank.

Putting things right

With all of the above in mind, I currently think that Starling should refund 50% of Mr F's loss, from and including the fourth payment. This is because Starling missed an opportunity to prevent Mr F's loss from this point, but Mr F also didn't act reasonably.

Whilst our Investigator considered that different rates of interest should apply to the funds which originated from Mr F's Starling account to his H account, I think the most pragmatic outcome here is to award 8% simple interest per year on the total refund being paid, from the date the payments were made until the date of the settlement. I say this because Mr F has suffered a deprivation of funds he otherwise would not have suffered, had Starling correctly intervened and prevented the scam from continuing.

My provisional decision

For the reasons I've explained above, I intend to uphold this complaint in part and tell Starling Bank Limited to:

- Refund 50% of Mr F's outstanding loss, from and including the fourth payment to the final successful payment, which I calculate to be £3,675.15 (50% of £7,350.30)*
- Pay 8% simple interest per year on the total refund amount, from the date of debit until the date of settlement, less any tax lawfully deductible.*

Mr F accepted my provisional decision and had nothing further to add. Starling did not respond.

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.

As neither party have provided any new comments or evidence for me to consider, my final decision is unchanged from the provisional findings I've set out above.

My final decision

For the reasons explained, I uphold this complaint in part and tell Starling Bank Limited to:

- Refund 50% of Mr F's outstanding loss, from and including the fourth payment to the final successful payment, which I calculate to be £3,675.15 (50% of £7,350.30)
- Pay 8% simple interest per year on the total refund amount, from the date of debit until the date of settlement, less any tax lawfully deductible.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr F to accept or reject my decision before 1 April 2024.

Meghan Gilligan
Ombudsman