DRN-3774958

Complaint

Mr C is unhappy that Bank of Scotland plc (trading as Halifax) won't refund him the money he lost as part of a safe account scam.

Background

Mr C has an account with Halifax. In May 2021, he was called by a man who claimed to be a Halifax employee and a member of its specialist fraud team.

Mr C was told that someone had visited his local branch and attempted to gain access to his account. He was told that CCTV footage showed that this individual didn't match Mr C's description. He was told that he needed to move his money into a "safe account" to make sure that it couldn't be accessed. He was also told that there was a suspicion of internal fraud by an employee of the bank. The caller explained that, if he made these payments in accordance with their instructions, he'd be assisting the bank with apprehending the employee responsible for the fraud.

Unfortunately, this wasn't a genuine request. Mr C was speaking with a fraudster. The fraudster reassured him that the request was genuine and suggested he reassure himself by searching online using the term 'Halifax fraud' – this would show that the number that Mr C had taken the call from was genuinely that of the Halifax fraud team.

Mr C wasn't aware that it was possible for a fraudster to "spoof" a phone number and make it look as if the call had genuinely been made from that number. Mr C made three payments (£24500, £9000, and £15000 respectively) and applied for loan of £24,500 between the second and third payment. Halifax has since agreed to refund the third payment. It says that it should've recognised the enhanced fraud risk given that the instruction was given so soon after Mr C had successfully applied for a loan. As I understand it, Mr C continues to make the loan repayments.

When making the first payment online, Mr C saw the following warning:

> *"[Name], do you know this person well? We'll never call you to tell you to move your money to another account. And we'll never call from the number on the back of your card. If you get a call like this, hang up the phone."*

Mr C proceeded with the payment despite the warning. He says that he doesn't recall seeing it. Nonetheless, he was asked to call the bank before the payment could be processed. As instructed by the scammer, he told the bank employee that the payment was being made to a builder in connection with works that had already been completed. During the call, he was asked several questions to determine whether there was a risk of a scam. The bank employee discussed the risk of rogue trader scams and email interception scams.

At the end of the call, the bank employee said *"I need to make it clear that it is very unlikely that we would be able to get this money back once it has left your account. Can you confirm that this is a genuine payment and it is being made on your own instruction and not because someone else has convinced you that this is what you need to do?"* Mr C confirmed that the

payment was genuine and so it was processed.

Mr C was told by the scammer that, after the payments had been made, he needed to visit his local branch where he had an appointment with the manager. It was only when he arrived at the branch and learned that no appointment existed that he realised he had fallen victim to a scam.

Halifax investigated but declined to pay Mr C a full refund. It conceded that it should've looked more closely at the third payment, particularly since it followed a loan application. But overall, it considered that Mr C had been given clear warnings about the risks of fraud both online and verbally. It said that its job in protecting him from fraud was made considerably more difficult because Mr C lied about the purpose of the payment. It also thought that Mr C should've found it strange to be asked to participate in an internal fraud investigation.

Mr C was unhappy with the response he received from Halifax and so he referred a complaint to this service. It was looked at by an Investigator who didn't uphold it. The Investigator thought that the warnings were sufficiently clear, and that Mr C should've recognised that this must have been a scam.

Mr C didn't agree with the Investigator's opinion. He said that he didn't recall seeing the specific warnings, but that he was in such a state of panic at the time that he might not have been able to process them and reflect on their contents.

Because Mr C didn't agree with the Investigator's opinion, the complaint was passed to me to consider.

Findings

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

I issued provisional findings on this complaint in August 2022. I explained my intended outcome in the following terms:

> *I've considered all the available evidence and arguments when looking at 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.*
>
> *In broad terms, the starting position at law is that a firm is expected to process payments and withdrawals that a customer authorises, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. However, where the consumer made the payment because of the actions of a fraudster, it may sometimes be fair and reasonable for the bank to reimburse the consumer even though they authorised the payment.*
>
> *The Lending Standards Board's Contingent Reimbursement Model code ("the CRM code") is of particular significance here. Halifax is a signatory to that code. It requires its signatories to reimburse customers who are victims of scams like this one in all but a limited number of circumstances. Halifax says that one or more of those exceptions are applicable in this case. I've dealt with each exception in turn below.*
>
> *Did Halifax give an effective warning?*

The CRM code says that, where a firm identifies a scam risk, it should take reasonable steps to provide its customer with effective warnings. To meet the standards required under the code, the warning needs to be (as a minimum) understandable, clear, impactful, timely and specific.

Mr C was provided with two warnings as part of the process of making his first payment – one was presented online and the second was given verbally when he called to request that the payment be released. The content of those warnings is set out in the background section above.

Effective warnings need to be impactful enough to overcome, or at least attempt to overcome, the typical features of the type of scam they seek to prevent. I agree that this warning was, broadly speaking, relevant to the complaint. Mr C had received a call apparently from his bank and he'd been asked to move his money.

It didn't say anything to give context to that statement – for example, Mr C wouldn't have realised that fraudsters might imitate the bank by creating a phony internal corruption investigation. It doesn't explain that fraudsters can spoof the bank's contact numbers. It's also prefaced with the question "do you know this person well?" – this opening remark isn't relevant to the scam that had targeted Mr C. I think this attenuated the impact of the wording that followed because it made it seem less relevant. It's also significant that he'd also been coached by the scammer to tell the bank that he was making the payment to a person that he did know.

The CRM code also says that an effective warning needs to include the appropriate action a customer can take to address the risk of a scam. This warning does say that Mr C should hang up, rather than continue with the call but it goes no further than that. I don't think that was sufficient to meet the requirements of the code.

I've also considered the verbal warning that was given when Mr C called to ask for the payment to be released. The initial questions that were asked weren't relevant to the scam, although I recognise that this was driven by the fact that Mr C gave false information when questioned about the purpose of the payment – something the scammer had insisted that he needed to do.

It's a commonly occurring feature of impersonation scams that customers are told that they're assisting with an investigation into potential fraud by a bank employee. This means the customer starts from a position of distrusting the genuine bank employee because of what they've been told by the fraudster. I don't think the warnings did enough to combat this distrust for the reasons I've explained.

At the end of the call, Mr C was asked to confirm that he wasn't making the payment because someone else had convinced him to do so. The questions he'd been asked hadn't flagged the possibility that this was in connection with a safe account scam and the question was presented in a way that would've appeared to Mr C to be part of a box-ticking exercise.

I don't find it surprising that he wasn't fully engaged with the content of the question or that it didn't raise any doubts in his mind about the legitimacy of the payment he was making. Overall, in this particular case, while I accept Halifax did take steps to warn Mr C about impersonation scams, I don't think the warnings Halifax provided were strong enough to break the spell of the type of scam Mr C fell victim to and so I'm not persuaded it provided effective warnings in compliance with the requirements of the CRM Code. This means the 'effective warning' exception does not apply.

Reasonable basis of belief

Halifax has also argued that a further exception applies under the code:

> *In all the circumstances at the time of the payment, in particular the characteristics of the Customer and the complexity and sophistication of the APP scam, the Customer made the payment without a reasonable basis for believing that … the person or business with whom they transacted was legitimate.*

I've considered this point carefully and I'm satisfied that he did have a reasonable basis for believing that the transaction was legitimate in all the circumstances at the time of the payment. I'm satisfied that he sincerely believed that the call he'd received was from a genuine Halifax employee. He took false confidence from the fact that the number that had called him was the same one that he found when carrying out an online search for its fraud team. I'm satisfied he had no knowledge that number spoofing was possible and so he took the assurances from the scammer at face value.

Since he was confident that he was genuinely talking to an employee of his bank, he was more likely to take seriously the claim that he was assisting them with apprehending a corrupt employee. Halifax has suggested that it was implausible that Mr C would be recruited to assist with a fraud investigation and so he should've recognised that this couldn't have been a genuine request.

But there is a significant asymmetry of knowledge in play here. There's no reason why Mr C would've known what processes Halifax would have in place to tackle the problem of internal fraud. To the layperson, I don't think this explanation was an inherently implausible one. I accept that Mr C gave several false answers to questions asked by the genuine bank employee. This made Halifax's job considerably more difficult. But he genuinely believed that the previous call with the fraudster was with Halifax. And he'd been coached into thinking that anyone he spoke to at the bank could plausibly be involved in committing fraud.

Overall, I'm not persuaded that Halifax has done enough to establish that Mr C made this payment without a reasonable basis for believing that he was transacting with a legitimate employee of the bank.

Should Halifax have done more to prevent the scam?

At the time Mr C made these payments, good industry practice demanded that Halifax have systems in place to spot unusual or out of character transactions or any other indicators that its customers were at risk of fraud. In some circumstances, it was expected to take additional steps before processing a payment so as to protect customers from the possibility of financial harm due to fraud.

Halifax clearly recognised that there was an enhanced risk of fraud associated with the first transaction because it did intervene. Unfortunately, I'm not persuaded it did enough during that conversation to protect Mr C from fraud.

Earlier in this decision, I explained why I didn't find that the verbal warning given when Mr C called up to unblock the first payment was sufficient. The call handler asked several relevant closed questions that were driven by the false answers Mr C had given about the purpose of the payment.

I think Halifax ought to have recognised the possibility that Mr C had been provided with a cover story or coached to not give honest answers to questions from the bank. If it had questioned Mr C in more detail about the payment and asked open questions, I find it likely that Mr C would've struggled to think on his feet to give convincing sounding answers. The coaching he'd been provided by the scammer wasn't detailed and so I don't think it would've required much probing for the bank employee to recognise that Mr C wasn't being completely open about his reasons.

Overall, I think that there was a missed opportunity to prevent the scam at the point of the first payment. I think that, if Halifax had responded appropriately at the time, Mr C wouldn't have made the two subsequent payments or applied for a loan to fund them. I find that these later events were a direct consequence of its failure to prevent the scam from the outset.

I recommended that Halifax compensate Mr C in the following way:

- *Cancel the loan agreement that Mr C took out under the direction of the fraudster.*
- *Refund to Mr C:*
    - *The payments Mr C made in connection with the fraud, except where they were funded by the proceeds of the loan.*
    - *The payments Mr C made in connection with the loan.*
    - *8% simple interest per annum calculated to run from the date the payments were made until the date Lloyds pays a settlement.*

Mr C agreed with my provisional findings, but Halifax didn't. Its response was detailed, but the key arguments it contained can be summarised as follows:

- It doesn't agree that the preliminary question displayed at the top of the warning that Mr C saw diminishes its effectiveness, particularly given that the warning was fairly brief.
- The warning was relevant to the scam in question because Mr C had been asked to move his money to another account. It unambiguously says that the bank will never do this.
- Mr C says he doesn't remember the warning, but it was interactive. It wouldn't have been possible for him to proceed with the payment without properly engaging with the warning.
- During the call between the bank and Mr C prior to the first payment being made, he gave an impression of confidence. There was nothing in his tone or demeanour to suggest a person at risk of financial harm.
- When making the first and third payment, Mr C would've known from the Confirmation of Payee result that he was sending money to accounts operated by a different bank. He ought to have been concerned by that.

I've reconsidered Mr C's complaint in the light of the further representations made by Halifax. However, I'm not persuaded to depart from the conclusion I set out in my provisional decision.

I accept that the warning contained some information that was relevant to the scam. If Mr C had processed it and reflected on its contents, he might have recognised that it was unlikely he was talking to a legitimate employee of the bank. He's said he doesn't particularly recall the warning and that it must have escaped his attention because he was being rushed through the process by the scammer.

But in any case, he was labouring under the misapprehension that the person he was talking to was an employee of the bank. He'd also been reassured that his account was in *"offline mode"* – and so none of the payment instructions he gave would really debit his account. It was simply a necessary part of the process for apprehending a corrupt employee. I think he'd have responded similarly to any information displayed on the screen as a result of the Confirmation of Payee process.

In any event, notwithstanding any obligations Halifax has to retrospectively reimburse scam victims under the CRM Code, it didn't handle its initial telephone contact with Mr C well enough and so missed the opportunity to prevent the scam from taking place. Halifax has said that Mr C didn't give the impression of someone who was at risk of financial harm during that call and that there was nothing in his tone or demeanour to indicate otherwise.

I don't find this to be a particularly strong argument. He wasn't making the payment under duress, so I wouldn't have expected him to sound nervous or as if he was under pressure. He'd been assured that, by following the instructions of the caller, his money would be safe, and he'd help to apprehend a corrupt employee of the bank at the same time. I wouldn't expect there to be anything in his external behaviour to suggest that he was at risk of falling victim to a scam.

As I described in my provisional decision, I find that the payment was out of character for the account. The bank employee he spoke to asked him a series of closed questions, but he really should've been asked one or two open questions to probe the explanation Mr C gave as to why he was making this payment. This would've been far more effective in identifying that Mr C had been given a very superficial cover story and that he'd really fallen under the spell of a scammer. I think that if Halifax had handled this call differently the deception would've unravelled, and Mr C would've been prevented from making the later payments and the loan application too.

I've also considered whether Mr C can be considered partially responsible for his losses here. In doing so, I've considered what the law says about contributory negligence but also borne in mind the fact that I must reach a decision based on what I consider to be fair and reasonable. And having done so, I'm satisfied that he shouldn't be considered partially responsible.

The scammers successfully convinced him he was talking with a senior employee in the bank's fraud team. This was primarily achieved by spoofing a genuine contact number. Not all customers have the same level of knowledge. Other customers might not have taken this claim from the scammer at face value on that basis or they might have required the scammer to do more to convince them that the contact was genuine. Nonetheless, I don't think the fact that Mr C was taken in by these claims means that he was negligent.

In the round, I don't find that Mr C should bear any responsibility for the loss by way of contributory negligence. He was the victim of a relatively sophisticated scam and I'm persuaded that he was unaware of the risks in making the payments he did. In view of Halifax's considerably greater expertise, I think it should've done more than it did to protect him.

Putting things right

Halifax needs to put Mr C in the position he would've been in if he hadn't made the three payments to the scammer or taken out the loan. In response to the provisional decision, Halifax pointed out that the loan agreement was settled in December 2021 and the third payment has already been refunded.

That means that in order to compensate Mr C fairly, it needs to refund the first two payments he made in connection with the scam and refunding any interest he paid on the loan up until the point a settlement is paid. It should add 8% simple interest per annum to these payments calculated to run from the date they left Mr C's account until the date any settlement is paid to him.

Final decision

For the reasons I've explained, I uphold this complaint.

Bank of Scotland plc trading as Halifax should now pay redress to Mr C in line with the guidance I've provided above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr C to accept or reject my decision before 23 November 2022.

James Kimmitt
Ombudsman