DRN-4096548

The complaint

Ms L complains that Bank of Scotland plc trading as Halifax says it won't fully refund the money she lost when she was the victim of a scam in 2021.

Ms L brings her complaint with the aid of professional representation, but for clarity in what follows I will refer throughout just to Ms L.

What happened

I should firstly note tha in the submissions made to this service, not all of the facts are consistent throughout. Therefore, in what follows, I have set out what appears to be the sequence of events as best as can be established given the evidence available to me.

Ms L met someone on a dating site, who I'll refer to as M. While she hadn't met M in person, she'd messaged him for a period of around three months. M told her he'd travelled to eastern Europe to buy gold and gemstones for his work as a jeweller. He'd had trouble getting these items shipped back to the UK and said his bank had frozen payments from his account. He asked Ms L to help.

Payment one

M first asked Ms L to make a payment of £40,000 — supposedly to a shipping company. Ms L attempted to send this by international transfer to a US company, making the payment on 14 September 2021 from her Halifax account using online banking. Halifax declined to make the payment and called Ms L to discuss it. She was told the bank was concerned about the risk of fraud. Ms L was questioned about the reasons for the payment.

During the call, Ms L told Halifax she was trying to help out a family member. She said this was her son, and he'd asked her to make the payment to help with his business in the US. She insisted she was happy to make the payment.

Halifax asked further questions and discussed the risks of various types of scams and the risk of losing her money. Ultimately, Halifax said Ms L would need to attend a branch in person if she wanted to make the payment. She was told at this point that if she'd been given another reason for the payment, she should be honest about this with the bank because it was trying to protect her.

Ms L later updated M about what had happened. M asked her what she planned to say to the bank about the payment when she went to the branch, and Ms L explained about the cover story she'd already used. Before Ms L visited the branch, she asked M to tell her his full name and home address, believing this would be an extra check.

Ms L visited a branch the following day, and it appears she stuck to the same story about the purpose of the payment. While the evidence of exactly what was discussed in the branch is limited, Ms L says it took nearly 30 minutes for the payment to be processed, and in chat messages with M says *"I am not sure about this. They are going through the dating scam thing".*

Ms L then appears to have identified that M was not on the electoral roll at the address he claimed was his home, and the real property didn't at all correspond with the pictures M had previously shared.

She reported the matter to Halifax that evening as a scam.

Payment two

Ms L nevertheless remained in contact with M. About a week later, M said there had been a problem with the shipment and more money was needed. She was asked to send a further £15,000 to the international payee, Ms M made this payment online on 21 September.

Payment three

M then said he'd been stopped at customs with some gold bars in his hand luggage. On 29 September, Ms L attempted to send a further £12,000. This time the payment was intended for a personal account in the UK, which Ms L was told was M's solicitor. Halifax blocked the payment and again contacted her to discuss it.

During this call, Halifax told her they wouldn't process the payment. She was told that she was being scammed. Ms L accepted this, and the payment ultimately wasn't sent. Ms L told Halifax's agent about the previous payment. However, once again her funds couldn't be recovered.

After another week, M asked for yet more money. Ms L didn't want to send any more. She told M that too many things he'd said didn't appear to be true. She thought she was being scammed. Her friends had told her to be careful of M.

M sent Ms L a screenshot appearing to show a bank balance of over £15 million as proof he could repay her. Ms L then agreed to make another payment.

She first attempted to make a £10,000 bank transfer online, but the payment was blocked by Halifax. Ms L then visited another Halifax branch location later the same day. This time, Ms L told the branch staff that the payment was going to her stepdaughter to pay her rent. She used the payment reference 'Mum'. The staff accepted Ms L's story and the payment was sent.

However, again Ms L began to realise she'd been scammed. She called Halifax to report the payment on 22 September.

Halifax's subsequent steps

Halifax was ultimately able to recover part of the funds Ms L had sent. In total this amounted to £8,408.64. But Ms L was left significantly out of pocket.

Halifax considered whether it ought to refund Ms L for the remaining loss. Halifax is a signatory of the Lending Standards Board's Contingent Reimbursement Model (the CRM Code) which provides additional protection to scam victims against the impact of authorized push payment scams. The CRM Code doesn't apply to international payments such as the first and second payments made here. But it would apply to the third payment Ms L had sent.

Halifax therefore considered the third payment under the CRM Code. It didn't think Ms L had taken sufficient care to check who she was paying and what for. So it wasn't obliged to reimburse her in full. But accepting a share of the responsibility refunded Ms L 50% of that

third payment (repaying her the sum of £5,000).

While the CRM Code didn't apply to payments one and two, Halifax still considered whether it might be responsible. Halifax didn't accept it was at fault for payment one and didn't think it could reasonably have prevented that loss. It did not reimburse Ms L for this payment.

However, the bank said it could have done more to protect Ms L when she was making payment two and said it would share equal responsibility for the loss. It refunded 50% of the value of that payment (repaying her the sum of £7,500).

In total, Halifax refunded £12,500. Taken together with the recovered sum of £8,408.64 this meant Ms L received back £20,908.64. But this left a loss of just over £44,000.

Ms L asked our service to look into the matter. Our Investigator thought Halifax had treated Ms L fairly, and in line with the CRM Code where the code was applicable. She didn't think there were any other reasons she could fairly ask Halifax to pay Ms L more than the bank already had. She thought Halifax couldn't have prevented Ms L from making payment one. For later payments, while Ms L had already realised this was a scam, she had continued to send money – so the Investigator thought it was fair that liability should be shared equally.

Ms L didn't accept the Investigator's findings. She said that Halifax should have questioned her further when she was making payment one in branch. And she argued that she had acted reasonably in making payments two and three so no reduction should be applied to the refunds Halifax had given – she should be fully reimbursed.

The investigator sympathised, but thought the outcome remained fair.

In light of this disagreement, I have been asked to review everything afresh and reach a final decision on the matter.

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.

In deciding what's fair and reasonable in all the circumstances of a complaint, 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. Where clear or unambiguous evidence is unavailable, I am required to reach my findings on a balance of probabilities – in other words based on what I find most likely given the information and circumstances before me.

Having done so I have reached the same outcome as that of our Investigator and for broadly similar reasons.

Firstly, Halifax has a primary obligation to carry out the correctly authorised payment instructions its customers give it. As a starting point, a customer will therefore assumed liable for a payment they have instructed to be made.

There is no dispute that Ms L authorised these payments, albeit having been deceived by a scammer into doing so. So, on the face of it she is liable for the resultant losses.

As I've mentioned above, the CRM Code can provide additional protection for the victims of APP scams such as this was. I'm satisfied that the CRM Code applies to payment three.

However, the first two payments were international payments. The CRM Code doesn't cover international transfers so I cannot fairly apply the terms of the Code to those two payments.

In what follows, I'll consider each payment in turn.

Payment one - not covered by the CRM Code

The first payment was an international payment, and as such the CRM Code does not apply.

Nevertheless, as a matter of good industry practice at the time, I'd expect Halifax to have been on the lookout for unusual or out of character transactions and intervening in the event it had concerns a payment might result in financial harm through fraud or scam.

I have listened to the relevant call recordings and considered the evidence provided by both sides about the circumstances leading up to this payment being made.

Based on what I've seen, I am satisfied that Halifax took substantive steps to protect Ms L. It initially blocked her attempt to make the payment online. Having done so, it then discussed the payment with Ms L. Unfortunately, Ms L provided the bank with a false story. It doesn't appear Halifax accepted Ms L's explanation at face value, and she was directed to a branch if she wanted to proceed.

I'm satisfied that there was likely a lengthy conversation between Halifax and Ms L when she visited the branch (as reflected in her messages to the scammer). She says in those messages that the bank had specifically warned her about romance scams. Reading those chat message indicates that the scammer had prepared Ms L for the questions she'd be asked in the branch, with the intent of preventing Halifax from being able to protect her from making the payment.

Of course, I can't know exactly what was discussed when Ms L visited the branch. But on balance I don't think Halifax could have prevented her from making this payment. I think she likely was questioned at some length by the branch staff but had prepared a thorough story with the assistance of the scammer. On the evidence I have, I therefore think it unlikely there would have been enough for the bank to reasonably have triggered the final stage of the banking protocol process. And in any event, I cannot ignore the fact that even after the scam first came to light, Ms L made further payments. I can't rule out the likelihood she'd have insisted on making payment one. The evidence doesn't lead me to find a causative failure on Halifax's part.

Overall, while I have carefully considered the arguments raised by Ms L, I don't think the bank could reasonably have prevented payment one from being made. When the scam was later identified, it appears Halifax took steps to recover the funds, although being an international payment there was limited scope to do so.

In short, I can't reasonably find Halifax was at fault in relation to this payment. That means I do not find the bank needs to accept liability for the resultant loss.

Payment two - not covered by the CRM Code

As with the first payment, payment two was international, and so the CRM Code is not applicable.

However, for this payment, Halifax accepts a share of the blame, and has refunded 50% of the amount Ms L lost. As the bank has already accepted fault here, I have not considered that point further. But I have given thought to whether it is fair that Halifax should apply a reduction of 50% in respect of contributory negligence on Ms L's part.

By this point, Ms L had been alerted by the bank that this was almost certainly a scam. And looking at the message history between her and the scammer, I think she'd realised this herself. I don't consider it was reasonable to have proceeded to make a further payment in this situation. All considered, I find it fair and reasonable that Halifax and Ms L should share the loss resulting from payment two equally.

Payment three - payment covered by the CRM Code

As with payment two, Halifax has accepted it was at fault in relation to the third payment Ms L made to the scammer. Unlike payment two, this was a domestic transfer, and so the CRM Code is applicable.

While the CRM Code offers additional protection to the victims of an APP scam, it includes provisions allowing a firm not to fully refund APP scam losses in some situations.

Relevant here, this includes an exception to full reimbursement where the customer made a payment without a reasonable basis for believing that they were paying for genuine goods or services, dealing with a legitimate person or business, or paying the person they believed they were paying.

Halifax says this exception applies here. It says Ms L made the third payment without holding a reasonable basis for believing what she did.

I have considered whether Halifax has acted fairly in seeking to rely on that exception.

I've carefully considered the evidence and arguments Ms L makes on this point. But I do not find it was reasonable even in the circumstances she was in to have made this final payment. I don't consider she had a reasonable basis for believing this payment was for a genuine purpose. I think this for broadly similar reasons to those I have explained in relation to payment two.

So, I find Halifax is entitled to rely on this exception to full reimbursement under the terms of the CRM Code in relation to this final payment.

As the bank has accepted it was at fault, and as it has established an exception to full reimbursement can be applied, the CRM Code says Halifax should refund Ms L 50% of her loss. The bank has already done so. Therefore I do not require Halifax to take any further steps here, it has reimbursed Ms L in line with the provisions of the CRM Code.

Overall

In saying this, I recognise that Ms L has been the victim of a crime here. She has been cynically exploited by a scammer, and I don't underestimate the impact these events will have had on her. Fraud is a horrendous crime, and romance scams in particular are especially cruel in nature.

But my natural sympathy for Ms L isn't a reasonable justification for holding Halifax responsible for everything that happened here. The primary cause of these events were the actions of the scammer. Having carefully weighed the evidence before me, I have reached my conclusions based on what I consider to be fair and reasonable in all of the circumstances. I do not find Halifax needs to do more than it has already done - I don't consider I can fairly require the bank to refund Ms L by more than the amount it has already repaid to her.

My final decision

For the reasons given above I do not uphold Ms L's complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms L to accept or reject my decision before 28 October 2023.

Stephen Dickie
Ombudsman