DRN-5038428

The complaint

Ms S complains that Bank of Scotland plc trading as Halifax 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.

In June 2021, Ms S met a man on social media who I'll refer to as "the scammer". The scammer seemed friendly and had photos on his profile. The conversation moved to WhatsApp, but when Ms S asked to meet in person, he said he was too busy with work and only agreed to a quick video call which ended abruptly.

After several weeks the scammer told Ms S that he did some trading. He sent screenshots of his investments and the profits he'd made and, eventually, he persuaded her to invest in cryptocurrency. The scammer encouraged Ms S to open an account with a trading platform which I'll refer to as "H". When she logged into the account, she could see live prices with graphs showing the rising stocks. She made an initial deposit of £300 and was guided by the scammer to open an account with a cryptocurrency exchange company which I'll refer to as "B".

The scammer asked her to first purchase cryptocurrency through B, and then load it onto an online wallet. Between 21 August 2021 and 3 September 2021, Ms S made two card payments to B and three faster payments to a P2P seller totalling £10,487.81. She also received a credit into her account for £1,044.98 on 22 August 2021.

Ms S was able to see her profit increasing on the trading platform and on 25 August 2021, she tried to make another withdrawal, but the scammer said she'd have to pay a withdrawal fee and commission. Desperate to withdraw her money, she made two further payments, but she realised she'd been scammed when she tried to borrow money from a friend, who told her she was being scammed.

Ms S complained to Halifax arguing that it had missed opportunities to intervene and to provide an effective warning. But it refused to refund any of the money she'd lost. It said the faster payments weren't covered under the Contingent Reimbursement Model (CRM) Code because she'd paid a genuine cryptocurrency merchant and received the cryptocurrency she paid for. And debit card payments aren't covered under the code. It also explained she didn't have any chargeback rights because she'd received the service paid for.

It also said that when it blocked a payment on 25 August 2021, she said she was sending funds to a family member and was told to speak to them before trying to send another payment. She then made a further debit card payment to B on 3 September 2021 when it was unable to provide relevant scam information because, again, she wasn't honest during the call.

Finally, it accepted she should have been given scam information after she was told the payments weren't covered under the CRM code and offered £40 compensation for poor customer service.

Ms S wasn't satisfied and so she complained to this service arguing that Halifax's intervention wasn't effective. She said it failed to provide effective or adequate warnings, which would have positively affected her decision-making at the time of the payments, and had it done so, she wouldn't have made the payments.

Her representative explained she'd been coached by the scammer to tell Halifax she was paying friends and family. They said Halifax should have contacted Ms S on 25 August 2021 when she made the payment of £3,000 (payment 2) because it was a high value payment to a new payee and the amount was unusual when compared to Ms S's normal spending. They said Halifax should have questioned her about the payment and if she'd said it was for friends and family, it should have spotted uncertainty in her response, and realised she'd been coached to lie.

Halifax explained that from the start of 2021 until the scam, Ms S sent £11,536.35 in faster payments, so it wasn't unusual for her to send faster payments. And if had intervened sooner, she'd have said she was paying friends and family, and she was paying a personal account in someone else's name, so this would've appeared legitimate.

Our investigator didn't think the complaint should be upheld. She agreed the payments weren't covered under the CRM code because the Code doesn't apply to debit card payments. And the faster payments were genuine payments to third party individuals who provided Ms S with the cryptocurrency she paid for.

She didn't think the first payment was unusual or suspicious. She said she didn't have enough information about what Halifax did when Ms S made the second and third payments, but she commented that even if it had intervened, it wouldn't have been in a position to provide an effective written warning. This is because the messages between Ms S and the scammer showed she'd been coached to lie, and when she transferred funds from Bank S to Halifax, she selected the payment reason as 'friends and family'. She also said the same thing when Halifax intervened on 25 September 2021 and the agent advised her to do more checks because the recipient was a business account.

Based on this evidence, our investigator thought it was likely Ms Shave selected the same transfer reason if asked before payment four, and this would have resulted in her being presented with a warning which wasn't relevant to the circumstances. So, the scam wouldn't have been stopped.

She further explained that she thought Halifax ought to have done more when Ms S made the fourth payment on 25 August 2021 as this was the third consecutive payment to a new payee that day, and while it wasn't high value, the cumulative total of the payments was unusual for the account. So, she thought Halifax had missed an opportunity to intervene. However, she didn't think an intervention before the fourth payment would have made any difference because she didn't think Ms S would have disclosed the real reason for the payment. In reaching this conclusion, she accepted Halifax had intervened later the same day and the agent refused to process a payment, but she was satisfied that as the fourth payment was to a personal account, paying friends and family would have been plausible, so the payment would likely have been processed.

Finally, our investigator didn't think Halifax had treated Ms S unfairly because there was no evidence it knew about her circumstances when the payments were made, so she was satisfied £40 compensation was fair.

Ms S has asked for her complaint to be reviewed by an Ombudsman. Her representative said that the payments she made on 25 August 2021 were highly unusual, particularly as one of the payments was to B. They also said money was coming into the account to cover each payment out, which is indicative of an investment scam.

They've argued that Halifax failed to effectively question Ms S about the payments or provide a relevant warning and it should have provided a tailored warning.

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 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.

The Contingent Reimbursement Model ("CRM") Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Ms S says she's fallen victim to, in all but a limited number of circumstances. Halifax has said the CRM code didn't apply in this case the disputed took place before the code came into force, and I'm satisfied that's fair.

I've thought about whether Halifax could have done more to recover the card payments when she reported the scam to it. Chargeback is a voluntary scheme run by Visa whereby it will ultimately arbitrate on a dispute between the merchant and customer if it cannot be resolved between them after two 'presentments'. Such arbitration is subject to the rules of the scheme — so there are limited grounds on which a chargeback can succeed. Our role in such cases is not to second-guess Visa's arbitration decision or scheme rules, but to determine whether the regulated card issuer (i.e. Halifax) acted fairly and reasonably when presenting (or choosing not to present) a chargeback on behalf of its cardholder (Ms S).

Ms S's own testimony supports that she used a cryptocurrency exchange to facilitate 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 exchange 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 Halifax's decision not to raise a chargeback request against either of the cryptocurrency exchange companies was fair.

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 his bank account, Ms S is presumed liable for the loss in the first instance.

There's no dispute that this was a scam, but although Ms S didn't intend her money to go to scammers, she did authorise the disputed payments. Halifax 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 Halifax 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 a genuine cryptocurrency exchange company. However, Halifax 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 did enough when she made the payments. If there are unusual or suspicious payments on an account, I'd expect it to intervene with a view to protecting Ms S from financial harm due to fraud.

The first payment was low value and so, even though Ms S was paying a cryptocurrency exchange, Halifax didn't need to intervene. Payment two was higher, but it wasn't identifiably linked to cryptocurrency. However, by the time Ms S made payment three, this was the second payment that day to the same payee and the cumulative total was £6,950, so I agree that Halifax should have intervened. I agree with our investigator that it should have asked Ms S about the reason for the transfer and then provided a written warning. But its likely Ms S would have said she was paying friends and family, so this wouldn't have been a warning tailored to cryptocurrency investment scam, and Ms S would have proceeded with the payment.

I also agree that Halifax should have intervened again before Ms S made payment four because by this time, the cumulative total for the day had risen to £9,750. This was the third payment she'd made that day to the same payee and the total sum of the payment was unusual for the account.

Halifax should have contacted Ms S and questioned her about the payment. But, based on the evidence of her communications with the scammer, what she said when she sent funds from Bank S, and what she said to Halifax before the fifth (attempted) payment, I think she'd have said she was sending money to friends and family (which would have been plausible) and the payment would have been processed.

So, while I do think Halifax missed opportunities to intervene, I don't think this represented missed opportunities to have prevented her loss.

Compensation

Ms S has said that she wants Halifax to pay her £300 compensation, but as the main cause for the upset was the scammer who persuaded her to part with her funds and I haven't found any errors or delays to Halifax's investigation, I don't think she is entitled to any more compensation.

Recovery

I don't think there was a realistic prospect of a successful recovery because of the time that had elapsed between the payments and the reporting of the scam. Further, Ms S paid an account in her own name and moved the funds onwards from there.

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 Halifax 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 6 December 2024.

Carolyn Bonnell
Ombudsman