DRN-4531838

The complaint

Mrs and Mrs P complain that Bank of Scotland Plc trading as Halifax didn't do enough to protect them from the financial harm caused by an investment scam company, or to help them recover the money once they'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.

Mrs P received a message on Whatsapp from someone who I'll refer to as "the scammer". The scammer explained she had Mrs P's details from when she'd previously registered her interest and asked if she was interested in a part-time remote job opportunity. She said she could earn £500 to £1,000 per week by conducting product reviews for a company I'll refer to as "N", explaining she would have to purchase the tasks by topping up her account with cryptocurrency.

Mrs P googled N and could see it was a legitimate company with a genuine website, so she decided to go ahead. The scammer told her to first purchase cryptocurrency through a cryptocurrency exchange company I'll refer to as "B" and then load it onto an online wallet so she could top up her account from there. Between 20 October 2022 and 1 December 2022, she made 25 payments to B totalling £52,759 using a debit card connected to her Halifax account. She also made fifteen faster payments to another account in her name which totalled £8,021.

Mrs P could see the product reviews related to products on N's website and she kept in touch with the scammer via WhatsApp and through an online portal. She was able to withdraw £60 and £188, which she put straight back into the platform, and she found the customer service department professional and helpful. But when she had completed 40 reviews, she tried to make a withdrawal and was told she didn't have enough credit and would need to make further payments, at which point she realised she'd been scammed.

Mr and Mrs P contacted Halifax with the assistance of a representative who argued it should have intervened and stopped the payments as they were linked to cryptocurrency. But Halifax said there was nothing it could do as Mrs P had authorised the payments and they weren't covered by the Contingent Reimbursement Model ("CRM") code as they were sent to accounts in Mrs P's name.

It said the debit card payments started off in small amounts and started to increase. It had contacted Mrs P on more than one occasion when she confirmed she was making the payments, she'd had previous dealings with B in June 2022, she was paying an account in her name, and the payments were in line with other activity from the account, so there was no cause for concern. It also said it had provided scam information including asking Mrs P to visit its website to keep up to date with scam information, which she chose not to do.

Ms P wasn't satisfied and so she complained to this service with the assistance of a representative. The representative said Mrs P had never purchased cryptocurrency before,

so the payments should have been concerning. They said that before the disputed payments, the largest payment was £3,500 for ground rent for a static caravan, and the account was otherwise used for bills, day to day shopping and savings. And her only income was her pension which was £700 per month.

They explained Mrs P was funding the payments by making very large transfers from an account in her own name, and on 21 November she moved £27,000 into the account, before sending almost all of it all out again, which is consistent with known scam behaviour.

They said Halifax should have contacted Mrs P and asked why she was making the payments and that she would have told it she was making the payments for a job. With that information it would have been able to identify this was a scam and provide specific warnings regarding cryptocurrency scams and advice on how she could protect herself.

Halifax said Mrs P could have done more to protect herself from the scam by conducting more checks. It said she wasn't given a contract or other employment documents and she didn't ask why she was being asked to pay money as part of the job opportunity. She was also communicating with the scammer via WhatsApp and the expected returns were unrealistic.

It said it blocked a payment on 9 November 2022, but it reviewed the activity and removed the block without speaking to Mrs P. On 11 November 2022, she contacted it claiming she didn't recognise any of the payments to B or the internal transfers into her account. And on 12 November 2022, she called again stating she'd been scammed and she was advised by the disputes team to contact B. It said payments were also blocked on 17 November 2022, but the blocks were removed after Mrs P confirmed the payments were genuine. And on 20 November 2022, Mrs P told the truth about the payments and was again told to contact B. The rest of the payments were made with no intervention.

It said Mrs P was dishonest on 11 November 2022 and on 12 November 2022, she told it she'd been scammed but went on to make more payments. So, even if it had questioned her further and given her scam education, it's unlikely she'd have told it the real reason for making the payments and she would probably have continued to make the payments.

My provisional findings

I explained the CRM Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Mr and Mrs P says they've fallen victim to, in all but a limited number of circumstances. Halifax had said the CRM code didn't apply in this case because the faster payments were to an account in Mrs P's own name and I was satisfied that's fair. It's also correct that the CRM code doesn't apply to debit card payments.

I also thought about whether Halifax could have done more to recover the card payments when they 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 (Mrs P).

Mrs P'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 Mrs P'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 was satisfied Mrs P '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, Mrs P is presumed liable for the loss in the first instance.

I explained it's not in dispute that this was a scam, but although she 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 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'd seen, the payments were made to a genuine cryptocurrency exchange company. However, Halifax had an obligation to be alert to fraud and scams and these payments were part of a wider scam, so I needed to consider whether it ought to have intervened to warn Mrs P when she tried to make the payments. If there are unusual or suspicious payments on an account, I'd expect Halifax to intervene with a view to protecting Mrs P from financial harm due to fraud.

Payments 1 to 13 were processed without any intervention from Halifax. I considered the nature of the payments in the context of whether they were unusual or uncharacteristic of how Mr and Mrs P normally ran the account, and I didn't think they were. All the payments were to legitimate cryptocurrency exchange that Mrs P had paid before and none of them were for particularly large amounts. So, I didn't think Halifax missed an opportunity to intervene.

On 9 November 2022, Mrs P paid £3,455 to B, and the payment was blocked, but released without a call to Mrs P. I considered whether this intervention was appropriate and based on the fact Mrs P had made payments to this payee on thirteen previous occasions, even though it was higher than the previous payments, I didn't think it was unreasonable for Halifax to have released it without contacting Mrs P.

The next interaction took place on 11 November 2022 when Mrs P called to tell Halifax she didn't recognise any of the payments to B dating back to June 2022, including the two pending payments of £15,750 and £7,381. She also said she hadn't made the large transfers into the account. I thought about whether the call handler could have done more the detect the scam during that call and owing to the fact Mrs P was dishonest, I was satisfied there was nothing the call handler could reasonably have said or done to detect the scam or to provide an effective warning at that point.

On 12 November 2022, Mrs P contacted Halifax again to discuss the payments of £15,750 and £7,380 she'd made the previous day. This time, she said she'd been scammed and the call handler put her through to the disputes team who said Halifax couldn't raise a claim on the payments and she would need to contact B.

Halifax hadn't produced a recording of the call Mrs P had with the disputes team, but, based on its description of what took place during the call, I thought it missed an opportunity to have prevented her loss. This is because I didn't think telling her to contact B was a

sufficiently robust response and it should have done more. It had a number of options including providing a robust scam warning, advice on additional due diligence and blocking payments to B, and I thought its failure to do this represented a missed opportunity to have prevented further loss.

Our investigator had said that because Mrs P misled Halifax on 11 November 2022, he thought she would have still misled it if it had intervened sooner. But I hadn't seen any evidence that she was dishonest on 12 November 2022, and she provided a lot of information about the scam on 17 November 2022 (when again she was told to contact B), so I thought she would have been open about the circumstances if properly questioned.

It had also been suggested that Mrs P would have continued to make payments to the scam because there are payments to B after the date she first contacted her representative. But she had explained those payments were made in relation to a recovery scam and I was satisfied that explanation is plausible.

Based on Halifax's description of what took place when Mrs P was passed to the disputes team and the fact she went on to make further payments to the scam, I wasn' satisfied it had shown that it did enough when she contacted it on 12 November 2022 to tell it she'd been scammed. And because of this, I thought Halifax missed an opportunity to have prevented Mrs P's loss and so I was minded to direct it to refund the payments Mrs P made after that point.

Contributory negligence

There's a general principle that consumers must take responsibility for their decisions and conduct suitable due diligence, but these types of scams can be very sophisticated and Mrs P had received two withdrawals quite early on. However, this isn't an excuse for failing to take reasonable care that she wasn't dealing with scammers. Mrs P had been contacted out of the blue by somebody who promised her £1,000 per week for doing product reviews and she didn't ask for any employment documents or question why she was being asked to pay for the tasks in cryptocurrency.

Further, I was satisfied she lied to Halifax when she contacted it on 11 November 2022 and that if she'd been honest on that occasion, the scam could have been prevented sooner. So, while I thought Halifax should have done more to protect Mrs P, I thought she should share some responsibility for the fact she made the payments in circumstances which should reasonably have given her cause for concern and without properly checking the job was genuine. Because of this I was minded to direct that the settlement should be reduced by 50% to reflect contributory negligence.

Developments

Both parties have indicated that they are happy to accept my provisional findings.

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.

Because both parties have indicated that they are happy to accept my provisional findings, the findings in my final decision will be the same as the findings in my provisional decision.

My final decision

My final decision is that Bank of Scotland trading as Halifax should:

- Refund the money Mr and Mrs P paid to the scam after the call on 12 November 2022, less any credits she received after that point.
- this settlement should be reduced by 50% to reflect contributory negligence.
- pay 8% simple interest*, per year, from the respective dates of loss to the date of settlement.

*If Bank of Scotland trading as Halifax deducts tax in relation to the interest element of this award it should provide Mr and Mrs P with the appropriate tax deduction certificate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr P and Mrs P to accept or reject my decision before 25 January 2024.

Carolyn Bonnell
Ombudsman