DRN-4324168

The complaint

Mr and Mrs D complain Bank of Scotland Plc trading a Halifax UK 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.

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 July 2018, Mrs D was contacted on social media by someone claiming to be a well-known American actor, who I'll refer to as "the scammer". Mrs D began to communicate with the scammer daily, exchanging details about their lives and families. The scammer told her he was getting divorced and that he had assets worth £350,830. He asked her to help him move the money so it wasn't part of the divorce settlement, in return for which he'd give her 10% of the money.

Between 30 August 2018 and 25 September 2018, Mr and Mrs D made thirteen payments to the scammer totalling £14,185.18. The first eight payments were under £1,000, and on 17, 20, 21, 24 and 25 September 2018, they made payments of £1,300, £1,000, £3,000, £3,800, and £2,000. The first six payments were made using a Visa debit card connected to their Halifax account, and the remaining payments were made via online transfer. Charges were applied to seven of the payments, many of which were international payments.

On 30 August 2018, Mr and Mrs D sent £209 to the scammer on the understanding it was to be the only payment. But he kept asking for money for various things such as shipping costs, delivery charges and fees to prove the money wasn't laundered. He put Mr and Mrs D in touch with his lawyer to help with the rest of the payments and said they might need to attend court to give evidence in his divorce proceedings.

They realised they'd been scammed when they went to the airport to collect a briefcase and it wasn't there. They tried to contact the lawyer and were told by the law firm he didn't work for them. They contacted Halifax but didn't receive a response.

When Mr and Mrs D complained to Halifax, it refused to refund any of the money they'd lost. It said it would try to recover the money from the overseas bank they sent it to, but there was no guarantee of success due to the time that had elapsed.

It accepted they were victims of an Authorised Push Payment ("APP") scam, which was covered under the Contingent Reimbursement Model ("CRM") code, but it said the code didn't apply because the payments were made before 28 May 2019. And it said it didn't intervene because the payments weren't out of character for the account, so it had no reason do any further checks.

Mr and Mrs D weren't satisfied and so they complained to this service. They said they didn't receive any scam warnings from Halifax, and they believed the scammer was who he said

he was because they felt they'd got to know him and that he'd provided a reasonable explanation as to why he needed the money.

They argued that if Halifax it had investigated the scam when they originally reported it, it might have recovered the money. And they said the payments were unusual because they only used the account to pay bills or to send money to personal accounts in their own name, so payments over £1,000 should have raised concerns and if they had any inclination that this was a scam, they wouldn't have gone through with the payments.

Mr and Mrs D's representative said Halifax should have intervened because they made 20 payments to four new payees totalling £14,185.18. They argued Halifax should have intervened, especially when they paid £850 on 14 September 2018 as this was an unusually large amount, to a new payee. Further, the payments were made in quick succession, which was an obvious fraud pattern.

They said Halifax should have contacted Mr and Mrs D and asked relevant probing questions and that it would have been apparent to a properly trained member of staff that they were falling victim to a scam, as its likely they'd have fully explained what was going on. It could then have provided a scam warning in response to which they would have chosen not to go ahead with the payments.

The representative explained Mr and Mrs D had held account for over 20 years and the payments represented a drastic change in activity, which should have raised concerns. Specifically, the account was used for payments to accounts in their own name or to pay bills, and there were very few payments over £100 in the months prior to the scam.

Halifax said Mr and Mrs D didn't do any checks prior to making the payments. It said Mrs D was contacted out of the blue by someone claiming to be a well-known actor and she didn't try to verify who she was speaking to or ask why she was making payments in circumstances where she'd been asked to help the scammer move his money.

It said it was unable to evidence the warnings she'd have been presented with due to the time that has passed, but the initial debit card payments weren't unusual as they were similar to other payments from the account. It accepted the payments increased in value, but not to the extent that it should have intervened. And the payments weren't completed in quick succession, with the balance was left healthy after each payment.

It reiterated the fact the payments were made before the CRM code and are a mixture of debit card and international payments, which aren't covered by the code.
Our investigator didn't think the complaint should be upheld. She accepted Mr and Mrs D didn't use this account often and mainly for specified purposes or one-off payments. She also noted that after funding their account and sending the payments, it would often be left with a low balance.

She said the payments dated 21 September 2018 and 24 September 2018 were the largest amounts, but she didn't think they were unusual as they followed the pattern of the previous payments. And as Mr and Mrs D didn't speak to or interact with Halifax, she didn't think it had missed an opportunity to intervene.

Our investigator said Mr and Mrs D were warned by other money providers that the payments may fraudulent. She also noted Mrs D regularly questioned the scammer over the legitimacy of the transactions but continued to make payment despite her doubts. So, she didn't think a warning from Halifax would have made a difference to the outcome. Finally, she was satisfied Halifax did what it could to recover Mr and Mrs D's money once it was aware of the fraud, but the money had already been removed.

Mr and Mrs D have asked for their complaint to be reviewed by an Ombudsman. They accept they were given warnings but explained Mrs D was suffering from moderate depression and that the scammer had played on that vulnerability. They maintain Halifax should have questioned the payments as they were large international payments which were totally out of character.

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 that Mr and Mrs D have been victims of a cruel scam. I know they feel strongly about this complaint, and this will come as a disappointment to them, so I'll explain why.

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 D say they've 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 payments 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 Mr and Mrs D's 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 (Mr and Mrs D).

However, the scheme sets the rules and there are specific time limits that must be applied. Those rules state that a claim can be brought no later than 120 days than the date of the transaction. In Mr and Mrs D's case, the claim was referred to Halifax after this time, so this wasn't an option for Mr and Mrs D.

I'm satisfied Mr and Mrs D 'authorised' the payments for the purposes of the of the Payment Services Regulations 2017 ('the Regulations'), in force at the time. So, they are presumed liable for the loss in the first instance.

Not every complaint referred to us and categorised as an investment scam is in fact a scam. Some cases simply involve high-risk unregulated investments that resulted in disappointing returns or losses. Some of these investments may have been promoted using sales methods that were arguably unethical and/or misleading. However, while customers who lost out may understandably regard such acts or omissions as fraudulent, they do not necessarily meet the high legal threshold or burden of proof for fraud, i.e. dishonestly making a false representation and/or failing to disclose information with the intention of making a gain for himself or of causing loss to another or exposing another to the risk of loss (Fraud Act 2006).

I've carefully considered the circumstances, and I am persuaded this was an impersonation scam. But, although Mr and Mrs D didn't intend their money to go to scammers, they 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. Transferring funds to international accounts is a legitimate activity. However, Halifax had an obligation to be alert to fraud and scams and these payments were part of a wider scam, so I need to consider whether it ought to have intervened to warn Mr and Mrs D when they 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 Mr and Mrs D from financial harm due to fraud.

The payments didn't flag as suspicious on Halifax's systems. I've considered the nature of the payments in the context of whether they were unusual or uncharacteristic of how Mr and Mrs D normally ran their account, and I don't think they were. The first eight payments were under £1,000 and while I accept these payments were to a new payee, they were relatively low value, and I don't think Halifax needed to intervene.

However, on 21 September 2022, Mr and Mrs D transferred £3,000 to the scammer. And on 24 September 2021, they transferred £3,800. These amounts were more than the previous disputed payments, and the other payments from the account in the months prior to the scam. However, by this time, Mr and Mrs D had already made several international payments, so this wasn't unusual. And while I accept £3,000 and £3,800 are large amounts, it's generally accepted that people do occasionally make larger payments. And they are not so high that the value alone should have triggered an intervention from Halifax, particularly as the amounts had increased gradually over the course of three weeks. So, while I accept the previous use of the account was very established, I don't think these payments represented a sudden change to the use of the account or that they warranted an intervention from Halifax. So, I don't think it missed an opportunity to intervene.

Overall, I'm satisfied Halifax took the correct steps prior to the funds being released – as well as the steps they took after being notified of the potential fraud. I'm sorry to hear Mr and Mrs D have lost money and the effect this has had on them. 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 Mrs D and Mr D to accept or reject my decision before 27 October 2023.

Carolyn Bonnell
Ombudsman