DRN-4629803

The complaint

Mr H complains that Bank of Scotland plc, trading as Halifax, won't refund him the money he lost to a scam.

What happened

Both parties are aware of the circumstances of the complaint so I won't repeat them in full here. But briefly, both parties accept that in around August 2021, Mr H met an individual on a dating app. Unfortunately, unknown to Mr H at the time, this individual was in fact a fraudster.

The fraudster proposed that they and Mr H take their conversation onto a different instant messaging app, which Mr H agreed to. Mr H has shared that he and the fraudster sent explicit photos and videos to each other, and Mr H believed they were building towards a future relationship. The fraudster then asked Mr H to pay for services he was receiving. Initially the fraudster asked for £80, but once Mr H sent this, she asked for a further £80, claiming she had to charge a higher fee. Mr H has explained he thought he would meet the fraudster soon to receive the services he paid for, however the fraudster would always provide excuses why she couldn't meet him.

Mr H continued to make payments to the fraudster in this way until October 2021. The fraudster told Mr H that the messaging app they were using fines her if she does not perform explicit requests that clients make - and that she therefore has a large debt with the messaging app. She also told Mr H that her daughter was in hospital. Mr H made over 60 payments to the fraudster to both financially support her and help her pay these debts. Mr H also purchased a phone on contract for the fraudster, which was collected by an individual Mr H understood was the fraudster's cousin. From reviewing later messages between Mr H and the fraudster, it seems the fraudster would frequently promise Mr H they would meet if he sent her funds, but they never actually did.

In November 2021, Halifax became concerned by Mr H's account use and requested he attend branch to discuss recent payments. While Mr H was in branch, Halifax invoked Banking Protocol and contacted the police, at which point it was uncovered that Mr H had fallen victim to a scam. Halifax raised a fraud claim concerning the payments Mr H had made to the fraudster.

However, while Halifax was investigating Mr H's claim, the fraudster's purported cousin (who I'll refer to as fraudster two for ease) contacted Mr H. He suggested he was also angry with the fraudster for issues she'd caused in his own personal life. He told Mr H that the fraudster was due to receive a pay-out for an injury she'd had, but that he was to receive the funds to his own bank account. Fraudster two suggested that if Mr H paid the solicitor fees, they could arrange for the fraudster's funds to be redirected to Mr H, to recover the money she'd scammed him of. From here began a second scam on Mr H, with Mr H making around 30 further payments to fraudster two to cover various fees he was told needed paying. While the second scam was occurring, Mr H also continued speaking with the first fraudster and sending occasional payments to her via fraudster two.

By the end of the scam, Mr H had sent around £43,000 to the two fraudsters. This was also funded through loans against Mr H's father's home with other banking providers and pension drawdowns. When Mr H saw the emotional impact this was having on his father, he stopped

making further payments, and became aware he'd fallen victim to a second scam, which was also raised with Halifax.

Halifax considered both Mr H's claims and whether it was liable to reimburse Mr H. Halifax considered that on four payments, where new payee details were entered, it could've provided better warnings to Mr H. Halifax therefore refunded Mr H 50% of these four payments it considered it shared liability on, totalling £405. It also contacted the beneficiary bank providers to attempt to recover Mr H's funds, but was only able to recover £1.94. However, for the remainder of Mr H's payments, Halifax didn't consider it ought to have done more. It considered the payments were generally low value and in line with Mr H's usual spending, and that when there had been a fraud concern, Halifax successfully invoked Banking Protocol to uncover the scam. Halifax also raised that, despite being in contact with Mr H to discuss the first scam, Mr H never made it aware that he was still in contact, and sending funds to, an individual linked to the first fraudster.

Halifax has explained that Mr H made a payment to fraudster two at the end of the first scam which was stopped by Halifax for further checks. When questioned, Mr H told Halifax this was a payment towards a skip but could now be cancelled. Halifax says it therefore had no reason to believe subsequent payments were potentially fraudulent.

Mr H disagreed with Halifax's response and so referred his complaint to our service. He considers that the volume of payments he was making ought to have caused Halifax to intervene sooner.

An investigator considered Mr H's complaint. He reviewed whether Mr H's complaint could be considered under the Contingent Reimbursement Model (CRM) Code which Halifax is a signatory of, which provides some protection to customers who are the victim of authorised push payment (APP) scams like this. However, he didn't consider the Code was applicable. He considered that the Code only covered payments that customers believed were for 'legitimate purposes' and based on the nature of this scam, he didn't consider the payments Mr H made were. In any event, the investigator thought that even if the CRM Code *was* relevant, Halifax couldn't be held responsible for Mr H's losses as Mr H didn't have a reasonable basis for believing the payments he was making were genuine.

Mr H disagreed with the investigator's view and so the complaint has been referred to me for a final decision.

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.

I'm very aware I've summarised this complaint briefly, in less detail than has been provided, and in my own words. No discourtesy is intended by this. Instead, I've focused on what I think is the heart of the matter here. If there's something I've not mentioned, it isn't because I've ignored it. I haven't. I'm satisfied I don't need to comment on every individual point or argument to be able to reach what I think is the right outcome. Our rules allow me to do this. This simply reflects the informal nature of our service as a free alternative to the courts.

I want to start by saying how very sorry I am to hear of the impact this scam has had on Mr H and his family. I want to assure Mr H that I don't underestimate the immense strain this must have placed on them all. However, my role is purely to look at the actions of Halifax and whether it ought to have done more to protect Mr H in the circumstances. Having done so, while I'm sorry to disappoint Mr H, I'm not upholding his complaint. I'll explain why.

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.

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 as a consequence 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.

When thinking about what is fair and reasonable in this case, I've considered whether the CRM Code applies to Mr H's claim and if so, whether Halifax should have reimbursed Mr H under its provisions - and whether it ought to have done more to protect Mr H from the possibility of financial harm from fraud. As it's questionable whether Mr H's claim is covered by the Code, I've also considered whether there are any other provisions under which Mr H should have been reimbursed by Halifax.

The CRM Code

As I've mentioned, Halifax is a signatory of the Lending Standards Board Contingent Reimbursement Model (CRM) Code. The CRM Code requires firms to reimburse customers who have been the victims of Authorised Push Payment (APP) scams, in all but a limited number of circumstances and it is for Halifax to establish that a customer failed to meet one of the listed exceptions set out in the CRM Code.

However, the CRM Code doesn't apply to all authorised push payments – the payment needs to meet the Code's definition of an 'APP scam', whereby:

- *'The Customer intended to transfer funds to another person, but was instead deceived into transferring the funds to a different person; or*

- *The Customer transferred funds to another person for what they believed were legitimate purposes but which were in fact fraudulent.'*

I've therefore considered whether both scams meet this definition for it to be considered an APP scam under the Code.

Is the first scam Mr H fell victim to covered by the Code and should Mr H be reimbursed under its provisions?

I think it's arguable in the first scam whether the payments Mr H made were for legitimate purposes. A large proportion of payments were made by Mr H in the belief that he was paying fines to someone who was coercing an individual into providing explicit services. However, it's also arguable that Mr H wasn't complicit himself in this coercion and was attempting to help someone out of a difficult situation.

However, even if I consider the payments Mr H made *are* covered by the Code, a bank may choose not to reimburse a customer if it can establish that*:

- The customer ignored what the CRM Code refers to as an "Effective Warning" by failing to take appropriate action in response to such an effective warning

- The customer made payments without having a reasonable basis for believing that: the payee was the person the Customer was expecting to pay; the payment was for genuine goods or services; and/or the person or business with whom they transacted

was legitimate

**Further exceptions outlined in the CRM Code do not apply to this case.*

Having considered the circumstances of the first scam holistically, I don't think Mr H had a reasonable basis for believing the payee was legitimate. Mr H has explained that the very first payments he made to the fraudster were fees to speak on a new messaging app and for services that he never received. He's explained he questioned why he needed to pay the fraudster a fee, as he'd already paid a fee to the initial dating site he'd joined, but the fraudster persuaded him to. Once he sent the first payment, the fraudster claimed she had to charge a higher fee, but then never met with Mr H to provide any services.

I think from the outset here, there were signs that things were amiss. The fraudster has insisted Mr H pay for fees that he doesn't appear to understand - and has then charged him for services she didn't provide. I therefore think there wasn't a basis for believing the fraudster was legitimate from the outset. I also think this is the case as the scam progressed. A large proportion of payments Mr H made were to pay apparent fines that the fraudster was receiving from the app they were speaking on – and yet from researching this app online, I can't see anything that suggests that this would be plausible. While the app is no longer in use, it appears to have been a standard instant messaging app, with some integrated features for dating. I've not seen anything that suggests more than this. I appreciate the fraudster went as far as creating a falsified email for the messaging app to confirm the fines – however again I don't consider it plausible that there would be an email support team to help receive illegal payments, and why the police couldn't have instead been involved to resolve this issue. Additionally, it's unclear why the fraudster would proactively choose to move her conversation with Mr H onto a messaging app that could fine her for not completing explicit requests and that she already held a debt with.

Mr H has explained that the fraudster repeatedly promised to meet him, then would make excuses why she couldn't. I think this also ought to have been a concern for Mr H. It seems to me unrealistic that despite forming a deepening connection, the fraudster would have to cancel meeting with Mr H on so many occasions, and ought to have caused Mr H to question whether the person he was paying was genuine.

I've then gone onto consider whether Halifax did - or otherwise ought to have - provided effective warnings to Mr H during the payments he made. The Code states that firms should provide an effective warning where they identify APP scam risks in a payment journey. Halifax provided a 50% refund for two of the payments made during the first scam, where a new payee was entered and Halifax provided a warning it didn't consider efficient. Having reviewed the payments Mr H made towards the first scam, while I appreciate the number of payments was vast over the full period, they were mostly relatively low value until the end of the first scam, at which point they became more moderate. I don't think the value of the payments were so significant that Halifax ought to have identified that they posed a higher fraud risk and provided an effective warning on this basis. However I do think the volume of payments Mr H was making, sometimes in one day, *was* unusual. So I've considered whether I think Halifax ought to have done more to question Mr H on this basis. Based on everything I've seen, I don't think it would be fair to conclude that had Halifax intervened sooner, this would have stopped Mr H incurring further losses to this scam. I say this because Halifax *did* intervene later in the scam and invoke Banking Protocol, resulting in Police intervention. However, in spite of this, Mr H continued speaking to the fraudster – and even sending her funds at times. Therefore, having considered the complaint holistically, I can't fairly conclude that had Halifax intervened sooner, either by providing effective warnings, or by stopping payments until it had further questioned Mr H, that this would've impacted the situation Mr H now finds himself in.

I therefore don't think Halifax has acted unfairly in how it has considered Mr H's complaint regarding the first scam – and it follows that I am not requesting Halifax does anything further to put things right for Mr H.

Is the second scam Mr H fell victim to covered by the Code and should Mr H be reimbursed under its provisions?

I think it's more clear cut for the second part of Mr H's claim that he was aware the payments he was making weren't for legitimate purposes. I say this because Mr H, by his own admissions, was under the impression that he was arranging with who he thought was the fraudster's cousin, to obtain money from her without her prior agreement or consent. I therefore don't think payments made towards scam two fall within the scope of the CRM Code. However, I have still considered whether Halifax ought to have done more in identifying signs that Mr H may be at risk of financial harm from fraud and intervening sooner.

Halifax has explained that the first attempted payment made to fraudster *two* was on the same day that Mr H logged his scam claim for scam *one.* However the payment was blocked at this time and Mr H did not call Halifax until two days later to remove the block. At this time, when questioned about the payment, he explained that the payment was to a construction company (which matched the recipient account holder's name) and was intended for a skip. However, he advised that he now planned to pay for the skip in cash and so the payment could be cancelled. Mr H didn't make a further payment to fraudster two until a few days later, at which point fraudster two was effectively an 'existing payee' and further payments weren't stopped. Again, payments to fraudster two, while moderate until the end of the scam, were frequent – so I've considered whether Halifax ought to have identified this as a potential scam risk and intervened to protect Mr H from the possibility of financial harm from fraud.

Again, even if I was to determine that Halifax ought to have intervened in these payments, I can't fairly conclude this would've made a difference here to Mr H's losses. At the time Mr H spoke to Halifax and advised them the initial payment was for a skip, he was aware that he had fallen victim to a scam from fraudster one, but chose not to disclose that this new payee was an apparent relative to the fraudster. Similarly he didn't disclose this in any subsequent correspondence with Halifax while it investigated Mr H's first claim. I therefore think it's more likely than not that, had Halifax stopped subsequent payments and questioned Mr H, he wouldn't have been honest about the payment purpose, thereby limiting how efficiently Halifax would've been able to stop the scam from proceeding. As I've already mentioned from scam one, it's also questionable whether, had Halifax uncovered this further scam, Mr H would've stopped making further payments, or continued to do so.

Did Halifax do enough to recover Mr H's funds, once it was made aware of the scam?

I also don't think Halifax could've done anything further to recover Mr H's funds from the fraudster after the scam had occurred. Unfortunately, by the nature of these scams, we usually expect fraudsters to remove funds received from the recipient account almost immediately after they're received. It's not clear how soon after the scam was raised that Halifax contacted the beneficiary accounts, but as the claims were raised days or more after the payments in question were made, I don't think any swifter action on Halifax's part would've made a difference here in whether funds were recoverable.

To conclude, for the reasons I've set out above, while I'm very sorry to disappoint Mr H, I don't think Halifax could reasonably have done more to protect Mr H from the scams he fell victim to. It therefore follows that I am not recommending Halifax provides further reimbursement to Mr H, either under the CRM Code, or under other regulatory provisions.

My final decision

My final decision is that I don't uphold Mr H's complaint against Bank of Scotland plc trading as Halifax.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr H to accept or reject my decision before 14 May 2024.

Kirsty Upton
Ombudsman