DRN-5188940

The complaint

Miss T complains that Bank of Scotland plc trading as Halifax ('Halifax') won't refund her the money she lost after she fell victim to an Authorised Push Payment ('APP') scam.

What happened

The background to this complaint is well-known to both parties, so I won't repeat it in detail here. But in summary, I understand it to be as follows.

In or around October 2023, Miss T was attempting to progress a visa application for a family member. Miss T had previously and successfully used a solicitor - who I'll refer to as 'T' - for visa applications and so sought their services again.

Believing everything to be genuine, between 31 October 2023 and 1 November 2023 Miss T made four payments totalling £12,500 to T's account. In February 2024, Miss T was then told that a further payment, for £14,000, was needed to be made towards the application. Miss T facilitated this payment by making the payment from the account she holds with Halifax to another account she holds with a different payment service provider. From there she sent the £14,000 to a different company account, which I'll refer to as 'R', who T was also a director of.

Having made these payments, Miss T was unhappy with the delays in the applications being progressed. She spoke with T's personal assistant to discuss matters and they introduced Miss T to somebody they knew, who I'll refer to as 'G' who they said would be able to help them with progressing the application. Miss T was aware that 'G' wasn't a solicitor, but as they had been recommended by T's assistant and as T had successfully completed work for her previously, she wasn't concerned about their legitimacy.

Miss T was told that she would need to pay a further £8,500 for the completion of the visa process. Believing things to be legitimate Miss T made the payments as requested. A full list of the transactions Miss T made, from her Halifax account, is listed below;

1.	31 October 2023	Faster Payment to T	£100
2.	1 November 2023	Faster Payment to T	£3,000
3.	1 November 2023	Faster Payment to T	£7,000
4.	1 November 2023	Faster Payment to T	£2,400
5.	2 February 2024	Faster Payment to own account	£14,000
6.	6 March 2024	Faster Payment to G	£500
7.	6 March 2024	Faster Payment to G	£3,500
8.	10 March 2024	Cash to G	£250
9.	10 March 2024	Cash to G	£250
10.	10 March 2024	Cash to G	£250
11.	10 March 2024	Faster Payment to G	£4,000

Miss T realised she'd been scammed when she didn't receive the visa, didn't receive a refund that she requested and contact with T and G ceased.

Miss T raised the matter with Halifax. Halifax is a signatory to the Lending Standards Board's Contingent Reimbursement Model (the CRM Code). This means Halifax has made a commitment to reimburse customers who are victims of authorised push payment scams except in limited circumstances.

Halifax looked into Miss T's complaint and upheld it in part. In summary, Halifax thought it was liable to refund Miss T the money she lost for payments 1-4 in the table above (payments to T totalling £12,500). Halifax also thought it should pay 8% simple interest on this amount and an additional £75 for the trouble and upset caused.

But Halifax didn't think it was liable to refund the remainder of the money Miss T had lost (payments 5-11). In summary, it didn't think it was liable as it thought Miss T ought to have carried out more checks before progressing with the further payments. Halifax was however able to recover £1,000 from the beneficiary account, which it returned to Miss T.

Unhappy with Halifax's response, Miss T brought her complaint to this service. One of our Investigator's looked into things, but didn't think the complaint should be upheld. In summary this was because she thought there was enough going on that Miss T ought to have had some concerns about the payments (transactions 7-11) that she was making. And she didn't think any better warning or intervention by Halifax would have made a difference. So, she didn't think Halifax needed to do any more than it already had.

Miss T didn't agree with our Investigator's view. As agreement couldn't be reached, the complaint has been passed 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 that 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 focussed 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.

Having thought about everything carefully, I've come to the same conclusions as our Investigator, and for much the same reasons.

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.

To begin with, Halifax has a primary obligation to carry out the payment instructions its customers give it. As a starting point, a customer will therefore be assumed to be liable for payments they have instructed to be made. There is no dispute that Miss T authorised these payments, albeit having been deceived into believing she was sending them for the purpose of obtaining visas. On the face of it, she is therefore liable for the resultant losses.

However, of particular relevance here, the CRM Code says that the victim of an APP scam such as this should be reimbursed unless the bank is able to establish that one (or more) of the limited exceptions to reimbursement can be applied.

Under the CRM 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*

Halifax hasn't disputed that the additional protections of the CRM Code should apply here. Under the terms of the CRM Code, the bank has reimbursed Miss T the first four payments, but it considers Miss T should be held liable for the remaining loss. (As Halifax has already recognised the first four payments should be refunded, I won't consider those payments any further as part of this decision).

However, not all payments that have been made here are covered by the CRM Code. That's because the principles of the CRM Code don't apply to cash withdrawals, nor to payments that are made to a consumer's own account and not to another person. So, when considering the table above – payments 5, 8, 9 and 10 are not covered by the CRM code as they involved a transfer to an account in Miss T's own name (payment 5) and cash withdrawals (payments 8, 9 and 10).

But, as well as the CRM code that I've mentioned, a bank also has wider obligations and a duty to protect its customers against the risk of fraud and scams so far as is reasonably possible. If, in breach of that duty, a bank fails to act on information which ought reasonably to alert a prudent banker to potential fraud or financial crime, it might be liable for the losses incurred by its customer as a result.

With this in mind, these payments need to be dealt with in two parts; those made to an account Miss T held in her own name and the cash withdrawals (which are not covered by the CRM code) and then those made by faster payment to UK bank accounts (which are covered by the CRM code). That's because different considerations apply to the different types of payment, so I'll consider Mss T''s and Halifax's liability for each of these payment methods separately.

Transaction 5 (£14,000 transfer to own account)

As I mentioned earlier, the CRM Code doesn't apply to all transactions made on a customer's account. Importantly, it doesn't apply to this payment, as it was going to an account in Miss T's own name.

But, while I find the CRM Code doesn't apply here, it isn't the full extent of the relevant obligations that could apply in cases such as this. Taking into account the law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider Halifax should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks, including anti-money laundering, countering the financing of terrorism, and preventing fraud and scams.

- Have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which banks are generally more familiar with than the average customer.

- In some circumstances, irrespective of the payment channel used, have taken additional steps, or make additional checks, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

In this case, I need to consider whether Halifax acted fairly and reasonably in its dealing with Miss T when she made the transfer, or whether it could and should have done more before processing it.

Did Halifax act fairly and reasonably when Miss T made the transfer for £14,000? (payment 5)

It's not in dispute that Miss T authorised the payment for £14,000, that she sent to an account she holds with another provider. Because of this Halifax had an obligation to follow her instructions. But there are some situations in which it should reasonably have had a closer look at the circumstances surrounding the transfers - as I've explained, I consider that as a matter of good practice Halifax should've been on the lookout for unusual and out of character transactions.

Based on what I've seen I think the payment for £14,000, ought to have stood out to Halifax as not being typical of how Miss T usually ran her account. So, I think it would be reasonable to have expected Halifax to have sufficiently questioned her about the payment. I've seen that Halifax did question Miss T about previous payments, but I'm not persuaded the conversation went far enough.

But this in and of itself, isn't enough for me to say that Halifax should refund Miss T the money she lost, I also need to be persuaded that sufficient intervention would have made a difference and prevented the payments from being made. Of course, I can't know for sure what would have happened had Halifax probed Miss T further. So, I have to base my findings on the balance of probabilities – that is, what I think is more likely than not to have happened, taking into account what I know.

Having thought carefully about this, sadly I don't think any further intervention at this point is more likely than not to have made a difference and stopped Miss T from making the payment. I'll explain why.

I'm persuaded Miss T would have been able to give plausible answers to any questions that Halifax could reasonably have been expected to ask. I think she would have been able to convincingly explain, that the payment was being made to an account in her own name. before being sent to a solicitor who she had dealt with successfully previously. Given the solicitor's she was paying also appeared legitimate and to be trading on Companies House, I don't think it's more likely than not that there would have been anything in the answers she gave that would have caused Halifax any further cause for concern.

So, I can't fairly or reasonably say that further intervention at this point would have made a difference.

Cash Withdrawals (payments 8, 9 and 10)

As mentioned previously, these payments also don't fall under the scope for the CRM Code.

When thinking about these payments, I don't think they would have appeared as so unusual or suspicious to Halifax – when compared to Miss T's typical account activity, that I could reasonably have expected Halifax to intervene and question them further before allowing them to be made.

It follows that I don't think Halifax has missed an opportunity to prevent the scam at this point.

The Faster Payments to UK Banks (payments 6, 7 and 11)

As stated above, these payments do fall into the scope of the CRM Code

However, the CRM Code won't always require a firm to refund payments in full. In particular, it says a firm can choose not to fully reimburse APP scam losses where the firm can establish that the customer made the transactions without having a reasonable basis for believing what they did - including that they were paying for a legitimate service. Halifax seeks to rely on that here.

When considering if Halifax has treated Miss T fairly in line with the CRM Code, I therefore must consider whether Miss T made the payments without having a reasonable basis for believing this was for legitimate purposes.

I have carefully considered everything Miss T has submitted, as well as the evidence submitted by the bank. Based on everything I've seen and been told; I'm not satisfied Miss T did have a reasonable basis for belief. I think there were a number of concerning factors here that ought to have made Miss T cautious and led her to complete more extensive research before making the payments she did, when making these three payments.

I say this because;

- Ahead of an earlier payment, Halifax had bought to Miss T's attention concerns it had about T, in that Companies House indicated it may be subject to strike off. While I might see why Miss T moved passed this, given T was at this point still seeming to provide a service. It was something that later ought to have been taken into consideration, when things didn't go as expected.

- While I can understand why Miss T might have employed T's services again initially, as she had successfully used them before. She seems to have taken what she was told about G at face value and I think she should reasonably have proceeded with more caution than she did. I say that as Miss T doesn't appear to have been given any explanations, nor has she asked for one, around why was she having to pay again (to G) for a service she had already paid for and not received.

- Alongside this, given by this point Miss T was also already having problems with T not delivering I think Miss T ought reasonably to have taken further steps to check who G was, and importantly how they were qualified to help her get things moving and what work they would be undertaking for the fee they were being paid.

- From the evidence I've seen, Miss T doesn't appear to have been provided with, nor asked for, any documentation from G, regarding the actual visa/payments she was making. Given the official nature of the service being provided, I think it would have been reasonable to have expected such documentation to be forthcoming.

- Alongside this, I don't think a legitimate supplier of these types of services would ask

for large sums of money upfront.

I can understand how in isolation any one of these things may not have prevented Miss T from proceeding. But when taken collectively I think there was enough going on here that Miss T ought to have acted far more cautiously than she did and should have had significant concerns about the transactions she was making. Overall, I find that Miss T ought to have done more to verify that the person she was dealing with was actually able to offer her a legitimate service around visa applications.

I've also considered whether Halifax providing better warnings would have made a difference. But for broadly the same reasons as mentioned above, I don't think they would have. I say that as I think Miss T would have moved passed any warnings, giving she's told us that she had no concerns that the people she was dealing with were anything other than genuine and I'm not persuaded any proportionate warning at this point would have made a material difference in preventing Miss T from proceeding with the payments.

Vulnerability under the CRM code

There are provisions under the code which might lead to a refund, even when a customer doesn't have a reasonable basis for belief. The relevant part of the Code says:

A Customer is vulnerable to APP scams if it would not be reasonable to expect that Customer to have protected themselves, at the time of becoming victim of an APP scam, against that particular APP scam, to the extent of the impact they suffered. This should be assessed on a case-by case basis.

I'm sorry to hear of the difficult circumstances that Miss T found herself in. I've no doubt that she has been through a very difficult time, and I don't doubt that the scam has impacted her further. But I've considered whether there were vulnerabilities present at the time to such an extent that Miss T was unable to take steps to identify the scam she fell victim to or to recognise steps she might take to test the legitimacy of what she was being told by the fraudster. To do so I must consider the details of the scam, Miss T's actions throughout, and the wider circumstances of what was happening.

I don't doubt what Miss T has told us. But having thought very carefully about everything Miss T has told us, I'm not persuaded that it would be unreasonable to expect her to have protected herself against the particular scam she fell victim to. And so, on balance, I don't find that Halifax need refund Miss T's loss under the vulnerability clause of the CRM code.

Recovery

I have considered whether Halifax did all it could to try and recover the money Miss T lost. Halifax was limited in terms of what it could do here; it could only ask the beneficiary banks to return any money that remained in the recipients' accounts. It needed to make enquiries quickly for the best chance of recovery. It is common for fraudsters to withdraw or move the money on as quickly as possible, which sadly was the case here, with only £1,000 able to be recovered and returned to Miss T.

Overall, I don't think Halifax missed an opportunity to recover any of the money Miss T sadly lost.

All things considered, I don't find that Halifax is liable to refund Miss T any more than it has already offered to her, under the terms of the CRM Code. In saying this, I want to stress that I am very sorry to hear about what happened to Miss T and I am sorry she has lost out here. She was the victim of a cruel scam designed to defraud her of her money. I appreciate that

she's lost a significant amount because of what happened.

But I can only look at what Halifax was and is required to do and I'm not persuaded that Halifax is required to refund her the full amount of her loss under the CRM Code and what it has already offered is fair and reasonable in the circumstances of this case. Nor that the bank was at fault in making the payments Miss T had instructed it to make or for any other reason.

My final decision

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

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss T to accept or reject my decision before 6 June 2025.

Stephen Wise
Ombudsman