DRN-4206474

The complaint

Mr C complains that Bank of Scotland plc trading as Halifax won't refund money he lost when he fell victim to an Authorised Push Payment (APP scam).

What happened

In March 2022 Mr C fell victim to a scam.

Both parties are aware of the circumstances of the complaint, so I won't repeat them all in great detail here. But in summary, it's not in dispute that Mr C was contacted by a fraudster, who had intercepted an exchange of emails he'd had with a solicitor, regarding a property Mr C was purchasing. The fraudster tricked Mr C into making the following payments that he thought were towards the property, but that were actually made to an account controlled by the fraudster;

15 March 2022	£25,000
16 March 2022	£25,000
17 March 2022	£25,000
18 March 2022	£25,000

Mr C has explained that he had been communicating with his genuine solicitors by email. He had previously successfully made a payment to his solicitors for £14,000 on 26 January 2022 (made up of a tester payment for £1, followed by a payment of £13,999), which was for a deposit towards the property. On 14 March 2022, Mr C received an email, from what appeared to be his solicitors genuine email address, saying that funds should be transferred into a trust account in readiness for completion, and that these should be paid from that day according to his daily online account limit.

Mr C has said considering the emails from the fraudsters were from his solicitors genuine address, included details of the correct balance due on the property and as they had been communicating by email for months, he thought he was genuinely dealing with his solicitor.

The scam came to light when, after the fourth payment was made, Bank of Scotland's fraud detection systems picked up that large amounts were leaving Mr C's account. It recommended that Mr C called his solicitor to check the payment instructions were genuine and when Mr C did this, it was confirmed that Mr C had been dealing with fraudsters.

Mr C raised the matter with Bank of Scotland. Bank of Scotland is a signatory of the Lending Standards Board Contingent Reimbursement Model (CRM Code) which requires firms to reimburse customers who have been the victims of APP scams like this in all but a limited number of circumstances. Bank of Scotland issued its final response on 17 May 2022, upholding the complaint in part. In summary it said it appreciated the emails (from the fraudsters) weren't significantly different for Mr C to notice they were intercepted, but that due to the warning it had given, it would have expected Mr C to have contacted his solicitors before he had paid. It added that genuine emails from Mr C's solicitors had warned of invoice related scams and that the bank had also provided relevant warnings, which Mr C had chosen to ignore.

Bank of Scotland added that it didn't think the first payment Mr C had made was significantly out of character, but that it became out of character when he made the three following payments over consecutive days. Bank of Scotland therefore thought it should be liable for 50% of the final three payments made and it refunded £37,500 to Mr C's account on 24 March 2022. Alongside this Bank of Scotland apologised to Mr C as he had to chase for a decision and was given incorrect information in branch, in recognition of this it compensated Mr C with £80.

Bank of Scotland also contacted the beneficiary bank (the bank to which the payments were made) to try and recover the money Mr C had lost, but it was only able to recover £63.49, which was returned to Mr C.

Unhappy with Bank of Scotland's response Mr C then brought his complaint to our service. Our investigator thought the complaint should be upheld in full. In summary she said it was the banks responsibility to provide Mr C with an effective warning, not the solicitors he was dealing with. She added that she didn't consider the warnings Bank of Scotland provided could be considered as effective. As well as this, on review of Mr C's usual account activity, she thought the first payment ought to have triggered an intervention by Bank of Scotland.

It was our Investigator's view that the emails from the fraudsters were from the genuine solicitors address and she didn't think any change in their format was enough to have alerted Mr C that something was amiss, or that they were so different that they should have aroused suspicion. Our Investigator recommended that Bank of Scotland should refund the remaining loss, along with interest.

Bank of Scotland didn't agree with our Investigators position. In summary, for reasons it had already set out it maintained that Mr C should share liability with it. But having looked at things again, it offered to refund Mr C 50% of all of the payments, meaning it was increasing its offer by a further £12,500.

Mr C didn't accept Bank of Scotland's revised offer. As agreement couldn't be reached the complaint has been passed to me for a 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.

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.

As I've mentioned above, the CRM Code provides additional protection for the victims of APP scams. I'm satisfied that the payments Mr C made fall within the scope of the CRM Code. But despite offering additional protections, the CRM Code includes provisions

allowing a firm not to reimburse APP scam losses fully where the firm can establish that the customer failed to take sufficient care when making the payment (often referred to as the exceptions to reimbursement).

Under the CRM Code, a bank may choose not to reimburse a customer if it can establish that*:

- 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.

- The customer ignored an effective warning by failing to take appropriate steps in response to that warning.

*There are further exceptions outlined in the CRM Code that do not apply to this case.

When assessing whether it can establish these things, a Firm must consider whether they would have had a 'material effect on preventing the APP scam'.

So, in deciding the fair outcome for this complaint, I must first determine whether Bank of Scotland has established these exceptions to reimbursement can be fairly applied.

I have carefully considered Bank of Scotland's representations about the warnings it gave and whether Mr C had a reasonable basis for believing the transactions to be genuine. But they do not persuade me to reach a different view to our Investigator. I'll explain why;

Effective Warnings

Under the provisions of the CRM Code, as a minimum, an "effective warning" needs to be understandable, clear, timely, impactful and specific. It must also provide information that gives customers a better chance to protect themselves against being defrauded and should include appropriate actions for customers to take to protect themselves from APP scams.

The CRM Code sets out minimum criteria that a warning must meet to be an 'effective warning'. In very broad terms, it requires that a warning will be capable of countering the typical features of the generic scam type identified during the payment journey.

I appreciate that the warning Bank of Scotland gave when Mr C made his first payment is, in part, relevant to the type of scam Mr C fell victim to. I'm persuaded the warning attempts to cover scams relating to a customer receiving an invoice or a bill. But the warning is not specific enough to the type of scam that Mr C was falling victim to, and that Bank of Scotland ought to have been aware of, given Mr C had told it the payment was for a house deposit.

The warning doesn't go far enough to make the risk of this specific scam really obvious to customers. It doesn't bring to life what this type of scam looks like, nor does it talk about the prevalence of this type of scam or explain how sophisticated the scams can be. For example – it doesn't explain that fraudster's emails appear to come from the same email address as the account they've hacked, that they can communicate with their victims on a genuine chain of emails or that fraudulent emails are usually received when a payment request is expected or that fraudster's emails can seem genuine and look the same or very similar to the person's they're impersonating. It also doesn't make it clear that any money sent as a result of a scam would be lost and likely irrecoverable, which is a requirement under the CRM code.

For broadly the same reasons, I don't find the warnings Bank of Scotland had said it presented Mr C with when he went on to make his subsequent payments could be considered as effective warnings. They are not specific to the type of scam Mr C is falling victim to.

I don't underestimate the challenge Bank of Scotland faces in providing warnings strong enough to break the spell in a sophisticated scam such as this. But the difficulty of meeting that challenge does not mean that the warnings given by Bank of Scotland here were sufficient or contained enough clarity to meet the minimum requirements in the CRM Code.

Overall, I'm not satisfied Bank of Scotland's warnings, met the requisite criteria here. I don't consider the warnings given were effective warnings as defined by the CRM Code. It follows that Bank of Scotland has not established it can fairly apply the exception to reimbursement relating to 'ignoring an effective warning'.

Even though I've concluded the warnings were not effective, I appreciate the warnings did, in part, have some relevance to the scam Mr C fell victim to. So, for completeness, I've gone on to think about whether Mr C reasonably moved past the warnings to proceed with the payment, given the particular circumstances of the fraud that he fell victim to.

Did Mr C have a reasonable basis for belief when making the payments?

I have carefully considered Bank of Scotland's representations about whether Mr C had a reasonable basis for believing the transactions to be genuine. But it does not persuade me to reach a different view. I say this because;

- Mr C wasn't aware of how email impersonation / intercept scams worked and hadn't previously been a victim to this type of scam. He was expecting to make a payment in regard to the property he was purchasing, so it wasn't a surprise for him to have received a request for payment. I can see why it would have been especially believable where the fraudsters knew the correct amount of payment that was required and the emails appeared to come from the same email address as Mr C's genuine solicitors.

- Bank of Scotland has argued that Mr C ought to have questioned why the funds had to be sent to a trust fund. Mr C has said he didn't think to challenge the change in bank details, because he assumed the purchase funds would be held separately. On balance, I can understand why he thought it was plausible for a solicitor to request the funds to be paid into a different account. It is not uncommon for firms to have different accounts for different purposes and I'm mindful here the funds Mr C was sending were ultimately intended to be for the owner of the property he was purchasing, rather than money for the solicitor. So I don't think it was unreasonable for him to have thought these funds may be held in a holding account.

- Bank of Scotland has said Mr C didn't try a tester payment first (as he did when paying a deposit to his solicitor's genuine account). Bank of Scotland is correct in that Mr C didn't make a test payment, as he had done previously. However, I don't think this takes away from the belief he had that he was dealing with his genuine solicitor and, in any event, it's unlikely that even if he had of done, it would have made a difference. It's likely the test payment would have been successful, so Mr C would have carried on making the payments regardless.

- I'm also mindful that Bank of Scotland has said the fraudsters initially provided Mr C with an incorrect sort code. But I'm not persuaded this in and of itself is enough for

Mr C to have reasonably suspected that things may not have been as they seemed. Mr C was then provided with an alternative sort code, from who he thought was the genuine solicitor. I think it's fair and reasonable that Mr C accepted the revised details, after all, he thought he was communicating with his genuine solicitors, and had no reason to doubt what they had sent him.

- I have seen a copy of the emails from the genuine solicitor and the fraudsters and I don't think there was enough of a difference to have alerted Mr C to the potential they had been intercepted. Which, Bank of Scotland has agreed with in its final response letter to Mr C, where it said it appreciated the emails weren't significantly different for Mr C to have noticed they were intercepted.

- Bank of Scotland has also pointed to a warning the genuine solicitors provided in a footer of emails it had sent previously, which advised customers to speak to solicitors before transferring money. It's important to note that the fraudsters emails did not contain the disclaimer. I don't think it's unreasonable that Mr C didn't notice the absence of the disclaimer and I don't think the absence is remarkable. It not being present also means that Mr C wouldn't have read the disclaimer just before making the payment. And it seems the fraudster deliberately removed the disclaimer/didn't include the disclaimer in their email to maximise the chance of the scam succeeding. I'm not persuaded the inclusion of the disclaimer, on earlier emails, means that Mr C didn't act reasonably, or made the payments without a reasonable basis for belief that the money was being sent to his genuine solicitor.

With all of the above in mind, in light of all the circumstances here, and in line with the requirements of the CRM Code, I'm not satisfied Bank of Scotland has been able to establish that when Mr C sent the payment he did so without a reasonable basis for belief.

Could Bank of Scotland have done anything else to prevent the scam?

In addition, I think Bank of Scotland ought reasonably to have done more to prevent this scam.

When looking at the activity on Mr C's account, in the months leading up to the scam I think the first payment he made, for £25,000, wasn't typical of how he usually operated his account. Although I can see Mr C did make a large payment to his genuine solicitors a couple of months previously, I'm persuaded that a payment for a significantly larger amount to a new payee ought fairly and reasonably to have led to Bank of Scotland wanting to satisfy itself that Mr C wasn't at risk of financial harm, before allowing the payment to be progressed.

Considering this, I think it's fair and reasonable to have expected Bank of Scotland to have intervened and questioned Mr C at the point he was making the first payment to a new payee and for it to have asked him some questions, before allowing the payments to be processed. Had it done so, I think the scam would've quickly unfolded and Mr C wouldn't have gone ahead with the first, or the subsequent payments. I'm persuaded this is supported by what happened when Bank of Scotland did contact Mr C after he'd made his fourth payment to fraudsters, when the scam was uncovered.

The relevance of this finding is that Bank of Scotland ought to have prevented the loss, rather than just reimbursed Mr C under the provisions of the CRM Code. It follows that Bank of Scotland should pay Mr C interest from the date of loss, rather than the date it decided not to refund him under the CRM Code.

Finally, I've considered the compensation that Bank of Scotland paid Mr C for the delays and incorrect information that he was provided. I recognise Mr C has fallen victim to a cruel and callous scam, which has impacted him and I don't underestimate how difficult a time this must have been for him. But I think it's important to highlight that the vast majority of the distress and inconvenience caused by this event was caused by the fraudster. And it isn't reasonable to hold Bank of Scotland liable for that. With this in mind I think the £80 Bank of Scotland has already paid is fair and reasonable in the circumstances.

Putting things right

For the reasons explained above, Bank of Scotland plc trading as Halifax should now;

- refund Mr C £62,500 being the remainder of the money he lost (less the £63.49 that was recovered).

- pay 8% interest on this amount, from the date of transactions to the date of settlement.

My final decision

For the reasons set out above, my decision is that I uphold Mr C's complaint against Bank of Scotland plc trading as Halifax and order it to pay the redress I have indicated above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr C to accept or reject my decision before 27 July 2023.

Stephen Wise
Ombudsman