

The complaint

Ms F complained about Bank of Scotland plc, trading as Halifax. Several transactions went through her Halifax credit card, which she hadn't made.

Ms F complained because she'd had to phone to report the transactions from abroad. She believed Halifax should have prevented the transactions, and she said she didn't feel safe banking with Halifax.

What happened

Ms F was working abroad in late November 2023. On 29 November, she saw four transactions on her Halifax credit card which she hadn't made. They had started on 12 November, and were all to an online food ordering and delivery company. Ms F rang Halifax from abroad to report them.

Halifax refunded the four transactions which had taken place from 12 to 26 November. These were for £22, £27.35, £60.99, and £20. Halifax also made interest adjustments relating to these, and it issued a new card.

Ms F rang Halifax again after she returned to the UK. Halifax told her that the fraudster had tried to use the replacement card. Halifax had blocked all these attempts, but it told Ms F not to use that card when it reached her. Halifax issued another replacement card.

On 3 December, there was another transaction on Ms F's account. This was for £5.75 and was to a travel organisation, but one which had the same parent company as the online food ordering and delivery company. Halifax refunded the £5.75 immediately, and blocked recurring payments from that retailer too.

Ms F complained.

In Halifax's final response to Ms F's complaint, it said that when Ms F had contacted Halifax on 29 November, it had refunded the disputed transactions to the online food ordering and delivery company. It had issued a new card, but it couldn't advise exactly how the fraud had happened. The transaction after the new card had been issued had been refunded, and a new card had been issued. Halifax also said it couldn't reimburse Ms F's call costs from abroad on 29 November.

Ms F wasn't satisfied and contacted this service. She said she'd discovered the fraud herself, and Halifax had treated it with contempt and had paid no heed to the distress and inconvenience caused, as well as nearly a whole morning on the phone from abroad. She said she wanted compensation for the cost of her phone calls, and for the distress and inconvenience she'd suffered. Our investigator asked her for evidence of the costs of her calls, but Ms F wasn't able to provide this. Ms F said she thought £100 compensation from Halifax would be fair.

Our investigator didn't uphold Ms F's complaint. She explained that although Halifax had systems in place to detect fraud, not all fraudulent transactions can be prevented. It had

stopped the card and refunded the transactions when Ms F reported them. The investigator also explained that the transactions had been set up as a Continuous Payment Authority (CPA). These can continue on a new card, even if a card is stopped and replaced. She said that the merchant was a genuine merchant, but Halifax had added the merchant to its CPA stop list.

The investigator also explained that being a victim of fraud isn't a bank's fault, and Halifax couldn't have foreseen this would happen while Ms F was abroad. She also pointed out that Halifax had lost out financially as a result of the fraud, because it had refunded Ms F.

Ms F wasn't satisfied. She said that:

- if Halifax had robust procedures in place, the fraud couldn't have happened in the first place;
- she had no idea how the fraud had been committed, and felt exposed and unsafe;
- Halifax had left her exposed to more fraud and extremely frightened.

Ms F asked for an ombudsman's 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 sorry to hear that Ms F was a victim of fraud. I know it can be upsetting and worrying, and I don't doubt that Ms F was very distressed by what happened. But it's fraudsters who are ultimately the cause of this unhappiness and concern, and sadly they can almost never be traced to make amends.

What I've considered in this decision isn't, therefore, whether Ms F was distressed, because I accept she was as a result of the fraudster's action. It's the much narrower issue about whether Halifax handled the problem correctly. Halifax – which ultimately picked up the bill for the fraud – also had an interest in preventing fraudulent transactions.

Ms F reported the disputed transactions on 29 November. Until then, I find that Halifax had no reason to know that the four transactions to the online food ordering and delivery company hadn't been authorised by Ms F. The transactions were authorised using Ms F's card details, and they were to a genuine retailer. Not every transaction to a merchant a customer hasn't used before is necessarily fraudulent. They were also for relatively small amounts, with the largest being £60.99. They also took place over several days, between 12 and 26 November. A fraudster with access to someone's card would typically carry out large transactions in a very short space of time, before the fraud could be spotted and the card stopped. I realise that Ms F says that Halifax should have prevented these transactions, but I find that Halifax couldn't reasonably have known they were fraudulent until Ms F reported them as such on 29 November.

I've looked at what Halifax did when Ms F reported the transactions. I can see that it refunded her in full, and also adjusted the related interest. It also blocked her card and issued a replacement.

I've then looked at what happened with the replacement cards. There were further attempted transactions on the first replacement card, all of which were blocked and didn't debit Ms F's account. The transactions had been attempted, despite being on a replacement card, because they were Continuous Payment Authorities (CPAs). CPAs are set up using card details, and give the merchant permission to take multiple amounts, not just one-off payments. They can be used for regularly recurring payments, and for taking different

amounts as and when the merchant needs – for example for membership or subscription accounts. As our investigator explained, CPAs can be transferred to any new card, without any new consent from the card holder.

CPAs are difficult for any card provider, such as Halifax, to spot. Card providers don't generally have a record of what CPAs are on an account. On their systems, CPAs often look the same as normal 'card-not-present' transactions (payments where the card details are entered remotely, without the customer or the physical card itself being presented, such as online purchases). With other repeating payments like standing orders and direct debits, the account provider has a record of what's due to go out. But CPAs don't usually have a paper trail. They are normally created online or on the phone. If the merchant wants to change the amount or frequency of payments, they don't have to give advance notice. And if a card provider doesn't know when the next payment is due or how much it will be, it's very difficult for them to stop it. This is particularly so because a CPA is linked to the account, not to the card – so changing the card doesn't stop the payments.

In Ms F's complaint, when payments continued to be attempted despite the change of card, this indicated that the payments had been CPAs. So Halifax put the online food ordering and delivery company on its list of blocked retailers for Ms F's account, and issued a replacement card. I find that in the circumstances of the fraudulent payments being CPAs, Halifax couldn't have realised this before the further attempts on Ms F's accounts.

I've also looked at the disputed transaction for £5.75 on 3 December. This was to a different entity, relating to transport rather than to online food ordering and delivery. This was why Halifax's block on the online food ordering and delivery company didn't prevent the transport transaction reaching Ms F's account. But the records show that Halifax refunded it immediately, and stopped further payments to that merchant too.

Ms F is concerned about how the fraud happened. I understand her concern, but neither Halifax, nor this service, can know how the fraudster obtained Ms F's card details, because that can happen in many ways. I also don't consider Halifax has any duty to pay for Ms F's phone calls to report the frauds. Halifax wasn't responsible for the frauds, and although Ms F was unfortunate in having to make a long-distance call to report them, that wasn't Halifax's fault.

In all the circumstances of this complaint, I find that Halifax couldn't have prevented the initial four payments. I also find that it did as much as it could to stop subsequent transactions, and it refunded all the disputed transactions with relevant interest. So I find that it acted fairly and reasonably, and I do not uphold Ms F's complaint.

My final decision

My final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms F to accept or reject my decision before 16 May 2024.

Belinda Knight
Ombudsman