

The complaint

Mr K complains Bank of Scotland plc trading as Halifax has refused to refund disputed transactions made from his accounts.

What happened

Mr K has a representative, but I will refer to Mr K throughout my decision for the sake of clarity.

Mr K was remanded into custody on 4 September 2021. At this point he says he lost access to his account debit cards and phone. As Mr K was unable to manage his financial affairs whilst in prison, he entrusted his account details to a friend who I will refer to as D.

On 28 October 2021 new debit cards and PINS were requested for Mr K's accounts. These were issued following a phone call to the bank.

In late 2022 Mr K contacted Halifax about a mixture of transactions he didn't recognise on his account. These consisted of debit card payments, cash withdrawals and contactless payments. Halifax wasn't aware of Mr K's incarceration, and reviewed the claim based on the information provided by M K and its technical data.

Halifax reviewed Mr K's concerns and issues a final response letter issued on 9 January 2023. This explains Mr K had highlighted transactions on his account that he didn't recognise from October 2021 to September 2022 and these totalled around £154,000. Halifax explained Mr K had told it that he had entrusted his accounts to D. This included asking D to order a new card and providing him with online banking log in details. Halifax declined the claim as although Mr K didn't make the transactions himself, he provided authority to D to use the card and PIN for the accounts. Halifax found Mr K's actions to be grossly negligent.

Halifax made the decision to end its banking relationship with Mr K which resulted in the closure of his personal and business accounts in December 2022.

Dissatisfied with this review Mr K referred the complaint to this service. Within his submissions to this service Mr K explained his version of events in detail. Mr K explained that he had provided D with his banking credentials in order for his personal and business accounts to be monitored. Mr K also provided D with access to his emails and phone SIM. Mr K explained that he at no point gave D permission to ask for a new debit card or PIN's. This also meant he didn't provide consent for transactions to be carried out on the accounts.

As part of his submissions Mr K put forward possible explanations for the transactions – this included D carrying them out himself, or a relative or D accessing the information and carrying out the transactions without D's knowledge. Mr K also thinks its possible someone was able to access the safe in his property and access his debit card and banking credentials.

An Investigator reviewed Mr K's concerns and gathered evidence from Halifax. This included account activity and technical information regarding the transactions that had been disputed. The Investigator didn't uphold Mr K's complaint. In summary, the following findings were made:

- Mr K has been inconsistent with what he has told this service and the bank about the disclosure of his banking credentials to D. But the evidence suggested D was given Mr K's online log in details, SIM card and then had access to debit cards and PIN numbers.
- The terms and conditions of Mr K's accounts clearly set out that credentials should be kept secure and not shared. Mr K breached these terms.
- Although Mr K's circumstances were unique as he was in prison there were other options available to him to ensure his personal and business accounts were effectively managed and kept secure.
- It wasn't Halifax's duty to ascertain who carried out the transactions.
- The service and support provided by Halifax was fair in the circumstances.
- There wasn't evidence to suggest Mr K had been treated differently by Halifax due to the nature of his offences.

Mr K disagreed with the outcome reached by the Investigator. Mr K asked to see some of the information the Investigator had relied on. Mr K also explained that he didn't request a new PIN for his debit cards. Mr K also explained that Halifax should've frozen the accounts given the activity on them and this would've limited Mr K's losses. Mr K also reiterated his belief that a relative of D carried out the transactions.

The Investigator provided Mr K with the information requested and also explained that his conclusions aren't based on whether the relative of D carried out the transactions. Rather the focus was on the relevant regulations and the account terms and conditions.

As Mr K disagreed with the Investigators review, the complaint was referred to an ombudsman for a final decision. Whilst the complaint was awaiting review Mr K provided further details of his complaint and losses incurred. In summary, Mr K explained his losses now stand at approximately £435,000. Mr K also reiterated his concerns about the fraud detection tools in place with Halifax and that this has contributed to his losses. Mr K believes Halifax's negligence is the key issue here, and the Investigator hasn't relied on clear and robust evidence.

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.

When considering what is fair and reasonable, 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 good industry practice at the relevant time.

Mr K is represented in this complaint, and I can see detailed submissions have been provided about the complaint and circumstances – both by Mr K and his representative. I'm also aware that I've summarised this complaint briefly. No discourtesy is intended by this. Instead, I've focussed on what I think is the heart of the matter here and the issues Mr K has reiterated his concerns about. If there's something I've not mentioned, it isn't because I've ignored it. This simply reflects the informal nature of our service.

Having looked at the complaint fully, my review of the evidence has led me to the same overall conclusions as the Investigator previously set out and for much the same reasons. I will explain why.

I can see Mr K feels very strongly about the complaint. That's clear from what he's said to both us and the bank. But from what's been said and provided so far, there's not much common ground about exactly what happened or how it might have happened. Where the evidence is incomplete, inconclusive or contradictory (as it is here), I reach my findings on balance – in other words, what I consider is more likely than not to have happened in the light of the available evidence and the wider circumstances.

The Investigator set out for Mr K the relevant rules and Mr K's account terms so I will not repeat them here. Under the relevant rules – the Payment Services Regulations 2017, Mr K is responsible for transactions he has authorised – either by doing them himself or giving permission for someone else to do them for him. The PSRs 2017 also set out that where a payment isn't authorised by the account holder, they may still be responsible for it if they've not been careful to follow the terms of their account or keep their personalised security details safe.

Essentially this means a customer should only be responsible for transactions they've authorised. Mr K says he didn't make any of the transactions in dispute. It isn't in dispute that Mr K didn't carry out the transactions himself given he was in prison at the time. However, Halifax can still hold Mr K liable for them if the evidence suggests it's more likely than not he authorised someone else to make them, or if he failed to keep his account safe – either by displaying a very high degree of carelessness or by intentionally failing to keep his card and PIN safe.

The transactions Mr K has disputed include cash machine withdrawals and online transfers. Halifax says the genuine card and PIN were used and the relevant verification procedures were followed. So, I'm satisfied the transactions were made with the genuine account information. But the regulations relevant to this case say this is not, on its own, enough to say Halifax can hold Mr K responsible for the payments he disputes.

A payment out of someone's account can only be treated as authorised if the payer has consented to it. In order to consider this effectively I've gone on to think about the circumstances around the transactions and whether Mr K gave his consent to the payments being made.

One of the difficulties in this case is the alleged fraud started many years ago and occurred over a long period of time. Mr K has provided his account of the actions he took when he was taken into custody. Mr K says he provided D with authority to deal with his financial affairs, but the exact details around exactly what details he disclosed to D have been inconsistent. I understand matters occurred many years ago, so I've thought carefully about what Mr K has said alongside the available evidence from Halifax and the account activity.

I think it's reasonable that Mr K would've disclosed online banking details to D – this would've been the main method available for the accounts to be monitored, and Mr K's submissions appear to generally accept that online banking details were disclosed. By providing access to these details Mr K was allowing D a significant amount of authority given many transactions and account related activities could be carried out with the online banking facility.

I've then gone on to consider the new debit cards and PIN that were ordered in late October 2021. Mr K says that he did not order these, and whoever had access to his account – be it D or a relative of D, had evaded Halifax's identification systems and managed to order

these. Halifax has provided its system notes from this time, and within these I can see its recorded that Mr K had given authority to D to manage his accounts. When looking at these notes alongside Mr K's comments, I find it most likely that Mr K was involved in the ordering of new cards for the accounts.

I must also highlight that the provision of online banking details would've allowed D to order new cards and a new PIN without the need for a telephone call. The disclosure of online credentials provided D with extensive control over the accounts. Mr K says that attendance at a branch with photo ID should be essential before a new debit card is issued. However, this was not a requirement for Halifax, and general industry practice is for customer's to be able to request new account cards and PIN numbers by phone and online banking. So, I don't find Halifax's decision to issue new cards in this manner was unreasonable.

I've also considered how the transactions that were in dispute were carried out. It appears some required a one-time passcode to be entered. This passcode would've been sent to the registered number on the accounts for Mr K. The technical information provided by Halifax shows the OTP was entered to the registered device. I'm satisfied this shows Mr K provided D with access to his device and this allowed the payments to be authenticated. Overall, looking at all the technical evidence available I find Mr K was grossly negligent with his account credentials, and this led to the losses he says he has incurred.

An overarching issue for Mr K is his belief Halifax should've done more to safeguard his accounts. I've thought about this carefully given Mr K's unique circumstances at the time. Banks like Halifax will have in place a range of measures to help detect fraud and financial crime to protect its customers' accounts and comply with its regulatory duties. There is no prescriptive method that each bank must use – instead it is for each business to implement what it considered robust measures to meet the requirements set out by the regulator and its legal obligations.

Firstly, I think it's important to highlight that Halifax was not informed of Mr K's imprisonment. This information only came to light after the transactions Mr K is disputing had been carried out. As explained above, I think it's most likely Mr K provided D with extensive information to allow access to his accounts. This meant that any transaction on the accounts was authorised using the relevant debit card, PIN or online banking details. This meant the normal safeguarding and fraud prevention measures Halifax had in place wouldn't have picked up this activity.

I must also highlight that there are instances where Halifax's security procedures were triggered. In a call made to Halifax on 23 December 2021 some of the information provided during call meant the advisor wasn't prepared to remove the telephone banking block that was in place. The caller was asked to attend branch, but as a call was made on 29 December 2021 with the correct information provided, this in branch visit was no longer required. I appreciate Mr K's frustration with the systems in place, however I think this example helps highlight Halifax was treating Mr K's account in the normal manner, and it took steps to ensure it was dealing with the correct individual.

I've also considered the transactions themselves. Mr K says there is a stark difference between the activity pre and post his imprisonment, but upon reviewing the activity, I don't think it is so unusual or extreme for Halifax's internal fraud triggers to be alerted. The transactions are spread across a long period of time, and the account didn't show any signs of financial stress. I understand Mr K says the cash withdrawals for example are excessive, but they were made using the account card and PIN, and I don't think the amounts withdrawn would've alerted Halifax to any potential issues. As a result, I don't think it would be reasonable to have expected Halifax to have taken any action or intervene with transactions that appear to have been authorised correctly.

Mr K says his imprisonment meant he had no option but to disclose some of his banking credentials to D. I appreciate Mr K felt he had limited options at this time, however but Mr K would've been able to provide a third-party mandate if necessary whilst he was imprisoned. This would've allowed a trusted third party to operate Mr K's accounts on his behalf. This option would've allowed Mr K to set limits or restrictions on what the third party was able to do – providing Mr K with significant control over the funds held. I also think its likely Mr K would've also been provided with information about how to manage finances whilst imprisoned.

Mr K says the support he received from Halifax when he detected the activity on his account was poor and he believes this is due to the nature of his conviction. Although I can't comment on every phone call and branch interaction Mr K has had with Halifax, I've considered the available evidence – including Halifax's internal notes provided and calls and I haven't seen information to support Mr K's view. Halifax appear to have dealt with Mr K in a professional manner and I can't see that it has treated him unfairly.

Overall, having considered everything, I'm not persuaded Halifax needs to compensate Mr K for the losses incurred. I realise that this is not the outcome Mr K was hoping for, and he will be disappointed by the decision I've reached. As such, I cannot fairly and reasonably require Halifax take any further action in relation to this matter.

My final decision

For the reasons explained above, my final decision is that I don't uphold the complaint.

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

Ombudsman