## complaint

Mr O complains that Bank of Scotland plc (trading as Halifax) has reported adverse information about him to CIFAS, the UK's fraud alert service.

## background

Halifax received a report from a different financial business stating that fraudulently obtained funds of £773 had been paid into an account it operated for Mr O. The money was credited on 6 November 2017. A transfer of £780 was then made by mobile banking from that account to another one of Mr O's accounts with Halifax. There were two cash withdrawals of £300 from this other account – one on 6 November 2017 at 21:02 and the other on 7 November 2017 at 02:51. A transfer of £100 was also made from the account to a credit card held in Mr O's name on 15 November 2017.

Halifax spoke to Mr O about the payments on 23 November 2017. Mr O told Halifax that he still had the card used to make the withdrawals. And that he hadn't told anyone his PIN but that it was in the 'notes' section on his phone which nobody should be able to access. He said he'd allowed someone to use his account in the past. Halifax considered the payments had been made by him and told him it was going to close the account in 60 days. Halifax reported to CIFAS that Mr O had used fraudulently obtained funds.

Mr O spoke to Halifax about this again twice on 24 August 2018 as the CIFAS marker was affecting his ability to get a job. It considered Mr O had given different information then about whether he had the card used to make the withdrawals or not and where his PIN was stored. Halifax still maintained that the CIFAS marker was correct. But it later agreed that in error it hadn't closed his account and it refunded all the subsequent charges and paid Mr O £112 in compensation.

Our investigator didn't recommend that the complaint about the CIFAS marker be upheld. He said that:

- Halifax had shown that the only device used to access Mr O's account through mobile banking had been registered to the account on 13 July 2017.
- To register it would've required a text to be sent to the number Halifax held for Mr O. This was the number he'd used to call it on in August 2018 about his complaint and the one this service had for him.
- His account had been accessed by mobile banking in October 2017 using a fingerprint and Mr O hadn't queried the related payments then made. On 6 November 2017 his account was also accessed online by using a fingerprint.
- Mr O hadn't been able to provide any evidence to show he'd lost his phone as he claimed or that he'd transferred his old number to a new phone.
- Mr O now said that it was years since he allowed an international student to use his account and that person was no longer in this country.
- Two balance enquiries were made about five minutes before the first cash withdrawal. That withdrawal was then made at a different cash machine about 0.6 miles away. So it was possible that someone had seen Mr O using his card and PIN and taken his card. However, the card had also been used to make a payment to a retailer just before the second cash withdrawal. He hadn't disputed that and there was no explanation of how his card was returned to him. His credit card had also been used on 7 November 2017 at a location less than 1.5 miles from the cash machines used that day.

- Mr O said that he still had his debit card when he spoke to Halifax about these payments on 23 November 2017.
- He was satisfied that Mr O had most likely consented to the payments and that they were authorised by him.
- He considered that the CIFAS marker was fairly registered as fraudulent funds had been received into Mr O's account and then used by him.

Mr O didn't agree. He said he wasn't a high risk customer and the CIFAS marker had a great impact on his ability to find employment. He didn't accept that he'd given inconsistent information about what happened. In his view, Halifax in sending him a cheque, had admitted negligence on its behalf. Mr O said he had done everything he could to get evidence that he had changed his phone and moved his number across. He did not think that this service had been fair and unbiased.

**my findings**

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

I need to take account of the Payment Services Regulations 2009. And to think about whether Mr O authorised the payments from his account. That's more than the payments being authenticated but would require him to consent to them. If he didn't authorise them then generally Halifax wouldn't be able to hold him responsible for them. I also need to consider whether the report to CIFAS was made fairly. On this point, Halifax needs to have more than a suspicion or concern. It has to show it had reasonable grounds to believe that a fraud or financial crime had been committed or attempted and that the evidence would support this being reported to the authorities.

I need to make clear that I don't consider that the error Halifax accepts it made by not closing Mr O's account at that time as it said it would do has any bearing on the substance of this complaint about the CIFAS marker. And I find I come to the same conclusions about this as our investigator and for the same reasons but I'll explain what I think about the evidence.

There is no dispute here that the funds (£773.00) paid into the account weren't for Mr O and had been reported by another financial business as fraudulent.

I'm satisfied based on the evidence provided that the related transfer was authenticated using Mr O's mobile banking and the withdrawals made when the chip on the genuine card was read and the correct PIN entered. The question I need to consider is the most likely explanation of how these funds were transferred to another account and then withdrawn. And whether Mr O consented to that or whether as he maintains an unknown third party made them without his knowledge or authority.

One key element to consider is the transfer between his accounts. I know Mr O says that his phone was lost. And that someone was able to use this phone and register it for online banking when it still had his number. To register it for biometric log in using a fingerprint Halifax say would've required Mr O's security information. There's no explanation how a third party would've been able to access that. As our investigator has said there were apparently genuine payments using mobile banking in October 2017. And I also don't think it's likely that someone with free access to Mr O's account would've waited until November 2017 before trying to take money from his account.

The other key element is the use of Mr O's card and PIN. I've listened to the call he had with Halifax on 23 November 2017. He very clearly states he still had the card for the account the withdrawals were made from. And he was asked to look at the card then in his possession and read out the last four digits of the number which he did correctly. So I find that compelling evidence he still had his card at that time.

But Mr O has given different explanations about his PIN and who had access to this. When he spoke to Halifax in November 2017 he said someone else had been using his account. He now says that person wasn't using his account by November 2017. He said he had his PIN stored on his phone in November 2017 and by August 2018 that he'd written it down on a piece of paper. The relevance of this is whether an unknown third party could've both found out his PIN and got access to his card. I'm struggling to see how this would've been possible.

To find that an unknown third party acting without Mr O's authority was able to make the transfer and these payments I'd need to think all of the following were most likely:

- That person was able to access his mobile banking account and decided not to use it to make fraudulent payments for several months but first make genuine payments for Mr O.
- That person was also able to get free access to Mr O's card on the day the fraudulent payment was made to his account. And somehow also to have discovered his PIN.
- That person was able to return the card to him without him knowing it had been used.
- By coincidence Mr O was using his credit card in a location close to where the disputed cash withdrawals were made on the same date.

These are not all findings that I'm able to make based on the available evidence. I consider he consented to these payments as he most likely made them himself.

*CIFAS marker*

Halifax says that it applied the CIFAS marker because Mr O received fraudulent funds into his account. So I've looked at whether Halifax was fair to apply the marker, based on the evidence it had, and the investigation it carried out. CIFAS guidance says the business must have carried out checks of sufficient depth to meet the standard of proof set by CIFAS. This essentially says that Halifax needs to have enough information to make a formal report to the police. And that any filing should be for cases where there are reasonable grounds to believe fraud or financial crime has been committed, rather than mere suspicion.
Having reviewed Mr O's account of events and the evidence Halifax has provided, I'm satisfied that Halifax had sufficient evidence for the CIFAS marker to be recorded. In coming to this view, I've taken into account the following reasons:

- Mr O received fraudulent funds into his account and didn't report this to Halifax at the time.
- He transferred the money to a different account. He withdrew most of the funds and used part of them to pay his credit card. So that he had benefit of this money.
- Halifax had grounds to believe that Mr O had used fraudulently obtained funds based on the evidence it had.

I appreciate that this will be a great disappointment to Mr O as the marker is having a detrimental effect on him. But given what I've said above, I don't think Halifax has treated

him unfairly in respect of the disputed transactions and recording the CIFAS marker. So I won't be asking it to do anymore.

**my final decision**

My decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr O to accept or reject my decision before 30 October 2019.

Michael Crewe
**ombudsman**