DRN-2899063

The complaint

Mr K is unhappy National Westminster Bank Plc ("NatWest") have applied a fraud prevention marker ("a Cifas marker") against him which is having an on-going impact on his finances.

What happened

Mr K contacted NatWest in June 2020 after discovering they had applied a Cifas marker against him.

The Cifas marker was applied by NatWest in December 2019 after they were made aware that Mr K's account had been in receipt of a fraudulent cheque. The cheque itself had credited Mr K's account on 9 December 2019. And in the following days, the value of the cheque, which amounted to just over £25,000, was spent via a series of chip and PIN card payments, as well as an online faster payment.

Mr K told NatWest that he didn't carry out any of this activity and would never commit any form of fraud. He also explained that the marker was having a serious impact on his life as he couldn't obtain additional finance to help his business progress.

NatWest reviewed Mr K's complaint and provided their final response in July 2020. They told him they wouldn't be removing the marker. Unhappy with their response, Mr K asked our service to look into his complaint.

One of our investigators reviewed the complaint. During the course of the investigation, Mr K told him the following:

- He didn't know how the fraudulent activity had taken place. He was unaware of the cheque crediting his account until January 2020 following a call with NatWest. At this point, he asked for his account to be closed.
- He didn't have his bank card with him – and hadn't used it since June 2019.
- The PIN for the card wasn't stored or written down anywhere at the time of the fraudulent activity – he had previously had the PIN recorded in his wallet, but he had lost this a year earlier. He also confirmed he hadn't told anyone his PIN.

NatWest also provided information for our investigator to consider. They said:

- They have no records of contacting Mr K in January 2020 and this wouldn't have been something they would've done. His NatWest account had already been closed – it had been closed the previous December following their internal review and so there wasn't an account to contact Mr K about.
- Although Mr K said he didn't know the whereabouts of his card, NatWest had not received any requests to cancel it or any reports that it had been lost or stolen.
- Based on their records, the last time the card was used was roughly nine months before the disputed activity. They thought it unlikely that someone could've obtained

Mr K's card and overseen his PIN at this point and waited a further 9 months to use it. Mr K had made no mention of how his PIN could've otherwise been known by a third-party either.
- Based on their online banking records, very similar IP addresses were used before and during the fraudulent activity to log in to Mr K's online banking. This indicated one person carried out the activity on the account – most likely Mr K.
- The device used for all online/mobile banking activity in December 2019 was the same device registered to the account in June 2019. Mr K had not disputed that it was him who registered the device and so NatWest thought it likely to be a device he had in his possession. This same device was used to check the account once the fraudulent cheque had been credited. And so NatWest believed it was Mr K who had checked the account and if the cheque crediting the account was unexpected, he would've reported it to them But he didn't.

Having reviewed the information available to him at the time, our investigator thought it reasonable for NatWest to have applied the Cifas marker. He was unable to identify how Mr K's card and PIN had been compromised alongside his online banking details - which would've been needed to log in to his account prior to the cheque being credited and to complete one of the transfers out too. As a result, our investigator thought on balance that it was most likely Mr K carried knew about or carried out the fraudulent activity – and was most likely aware of the fraudulent cheque which credited his account too.

Mr K disagreed with our investigator's findings and he provided some further information that he hadn't provided previously:

- Mr K said he had used his card shortly before the disputed activity took place – for a series of balance enquiries carried out on 3 December 2019 and he believes someone may've been able to see him enter his PIN at this point. He accepts he previously told the investigator he hadn't used the card for a while but said he didn't think about the possibility of balance enquiries when he was originally asked the question.
- Mr K also confirmed that he reset his online banking credentials on 3 December 2019. He confirmed this was done via the same device that he had used when he'd last accessed his online banking back in June 2019. Mr K also confirmed his online banking could be accessed via a passcode only.
- Mr K said he had all of his banking security credentials (including his online/mobile banking information and security passcodes) were written down in a small diary which was located in his vehicle. The same vehicle was accessible to several people he worked with at the time. Mr K also said that these same people often used his mobile phone to help complete certain jobs. As a result, Mr K believes one of these people could've accessed his mobile phone and gained entry to his account using the information contained in his diary – which they also had access to when in his car. Mr K accepted he didn't previously mention this but said he didn't feel it was relevant initially.
- Mr K believes someone is now impersonating him as he's received communication about a car which he says doesn't belong to him.
- Mr K also questioned why NatWest hadn't questioned the cheque crediting his account in the first place – given this was different to the account's normal activity.

Our investigator reviewed the complaint again and considered the new information provided by Mr K. However, his view remained the same and he didn't recommend the Cifas marker be removed. He highlighted Mr K's inconsistent version of events. And he remained of the opinion that it was unlikely that a third-party could've obtained everything needed (Mr K's

genuine card, PIN and online/mobile banking details) in order that they could carry out the disputed activity without Mr K's knowledge.

Mr K again disagreed with our investigator's view and requested an Ombudsman review his complaint. As an agreement has not been reached, the case has now 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.

Having done so, I agree with the outcome reached by the investigator. I'll explain why.

The marker that NatWest has applied is for misuse of facility. In this case, this means using the account to receive and then spend fraudulent funds. For NatWest to record this marker, they don't need to be able to prove beyond reasonable doubt that Mr K is guilty of the offence of fraud. But they are expected to be able to demonstrate that there are reasonable grounds to believe that a fraud or financial crime has been committed or attempted. Practically what this means is that NatWest must first be able to demonstrate that the funds that entered Mr K's account were fraudulent funds – and not part of legitimate activity. And secondly, they will need to have robust evidence that Mr K was deliberately dishonest in his activity – including allowing his account to be used for fraudulent activity.

With these considerations in mind, I've first thought about the funds themselves. NatWest has been able to provide evidence of it being contacted by another bank who explained that one of its customers had a fraudulent cheque credited into Mr K's account. Given the detail provided by the third-party bank, as well as the fact that Mr K has insisted he has no entitlement to these funds and wasn't even aware of them entering his account, I'm satisfied it is more likely than not the funds which credited Mr K's account were as a result of fraud.

I've then thought about the second element as to whether I believe Mr K was deliberately dishonest in his use of the account to the point it was reasonable for NatWest to escalate its concerns to Cifas.

From what I've seen, I'm persuaded it was reasonable for NatWest to do so. This is because:

- On balance, I'm persuaded it's most likely Mr K knew that fraudulent activity was about to take place on his account. I say this because I can see that someone logs in to Mr K's online banking on numerous occasions during the 9th, 10th and 11th December 2019. This suggests to me that whoever is accessing the account is aware that funds are about to be credited to it and is monitoring the account for their availability. The multiple successful log-ins to Mr K's online banking are completed using the same device that Mr K has confirmed he used to re-register for online banking roughly a week earlier on 3 December 2019.

  I acknowledge what Mr K has said about people he worked with being able to access his phone during this time as well as potentially having knowledge of his online banking details – which he says were stored in his diary in his vehicle. But given that the evidence shows that whoever had access to Mr K's device and online banking, was able to access the device across multiple days and at various times – I'm not persuaded that a third party fraudster would've been able to access Mr K's device

and login to his online banking on multiple occasions, at considerable risk to themselves, without him noticing and becoming aware of what was going on.

In addition to this, I note there are also successful log-ins to Mr K's online banking after all of the disputed activity has been completed. If a third-party had indeed carried out all of the disputed transactions, they would've known all the money had been spent. There would've been no need to access the account any further and once again, risk their exposure. And so I'm persuaded it's more likely than not that Mr K was the one who was accessed his online banking – yet he didn't report any of the fraudulent activity on the account to NatWest.

- I'm also persuaded it's most likely that Mr K was also the one to authorise (in some capacity) the transactions that allowed the fraudulent funds to leave his account. Mr K has said he used his card for balance enquiries on 3 December 2019. So I'm satisfied the card hadn't gone missing and was in Mr K's possession at this point. The card is next used in the middle of the night on 10 December 2019 for further balance enquiries at a location which is only a matter of minutes away from Mr K's address. By this point, the fraudulent cheque had already credited the account (something which would've been apparent as a result of both the balance enquiries and also the frequent online banking log-ins which had taken place on 9th and 10th December 2019 as well).

  However, it's then a further 15 hours before the card is finally used for the now disputed transactions – some of which also take place in locations only a matter of minutes away from Mr K's address. If a third party (without Mr K's knowledge or consent) had been able to take Mr K's card at some point between 3 and 10 December 2019, I'm not persuaded they would've waited such a substantial period of time before starting to utilize the funds in the account. The longer they wait, the bigger the risk that Mr K would've noticed his card was missing or that his account balance had suspiciously increased substantially – and that he would've reported the matter to NatWest and the fraud would've failed. And so I'm satisfied that had this balance enquiry been carried out by a third-party fraudster, they would've started to use the funds straightaway in order to avoid this happening. Yet whoever made the balance enquiry appears to have been confident that they would continue to have access to the account and the funds in it.

- NatWest has also been able to evidence that the disputed cheque was dated 3 December 2019. This happens to be the same day that Mr K decided to use his bank card for the first time in several months, as well as re-register for and access his online/mobile banking again. It is unusual that of all these things would happen on the same day – especially as the account had not been used for many months prior.

- Overall, in order to be satisfied that Mr K's version of events is most likely, I'd have to be persuaded that an unknown third-party was able to gain access to Mr K's genuine card and PIN (which he initially said wasn't written down) in order to pay a fraudulent cheque into his account in branch. I'd then have to be satisfied that the same third-party was then able to access Mr K's online banking via his own mobile phone on multiple occasions across numerous days without Mr K noticing.

  I'd also have to be persuaded that they were doing so to check the fraudulent cheque had been credited (which presumably they would've already known had they paid it in), all whilst either keeping hold of Mr K's card, or risking returning it and taking it again to do the balance enquiries. I'd also have to be satisfied that this third-party, who appears to have been very vigilant in checking when the money entered the account, waited 15 hours before accessing it. Once again, all without Mr K noticing

his account is being used. And all of the above is taking place in the same week Mr K started using the account again and had re-instated his mobile banking. On balance, I agree with NatWest that this seems unlikely.

I also want to address the question surrounding the phone call from NatWest that Mr K says alerted him to the cheque in January 2020. I've seen evidence from NatWest that shows it issued a letter to Mr K in December 2019 to explain his account would be closed. There's no indication Mr K questioned this account closure at the time. Instead, Mr K said that the first contact he had with NatWest was when he received a call from them in January 2020 – and it was at this point *he* asked for the account to be closed. However, I'm not persuaded this was what most likely happened.

The evidence shows that Mr K's account had already been closed in December 2019. So if Mr K had asked for the account to be closed in January 2020, I'd have expected NatWest to tell him that this had already happened. I'd have also expected Mr K to challenge why the account had already been closed in December 2019 when he received the letter stating as such – presumably this wasn't something he was expecting and he had just started to his account again. But this doesn't appear to have happened and Mr K doesn't get back in touch with NatWest until June 2020.

NatWest have also shown that they have no evidence of a call taking place in January 2020 and it doesn't make sense that NatWest would need to get in touch with Mr K after December 2019 – they'd already closed his account and applied the Cifas marker. They've also provided evidence of their call records which show no inbound or outbound calls to the phone numbers NatWest hold for Mr K (including the same one used to re-register the mobile banking on 3 December 2019).

Taking all of the above into account, I'm persuaded, on balance, that NatWest had enough evidence to meet the burden of proof required by Cifas in order to add the marker against Mr K. This is because I'm satisfied there's enough evidence to say the money sent (via cheque) to Mr K's account and subsequently spent was most likely because of fraud. In addition to this, I'm also persuaded it's most likely Mr K has helped to facilitate this and therefore acted dishonestly with NatWest. As a result, I don't think it's fair to ask NatWest to remove the fraud marker on this occasion.

My final decision

My final decision is that I won't be upholding this complaint against National Westminster Bank Plc.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr K to accept or reject my decision before 2 March 2022.

Emly Hanley
Ombudsman