DRN-3837944

The complaint

Miss M is unhappy that Capital One (Europe) plc ("CO") placed a fraud markers against her name.

What happened

Miss M says that she applied for a credit card with CO. After initially being accepted for this, the product was later withdrawn as CO believed the application was fraudulent and Miss M was being impersonated. CO also registered fraud prevention markers against Miss M's name.

Miss M contacted CO and assured it that she was legitimately the person applying for the credit card. She supplied her driving licence and a residence permit as identification to support this.

CO reviewed the information presented but maintained its position on the application and the fraud markers placed.

Miss M contacted our service as she remained unhappy with CO's decision. An Investigator reviewed the evidence provided by both parties but felt CO had made no error. Broadly, the Investigator concluded that there were sufficient risk factors that had been identified at
Miss M's home address that meant the application was fair.

Miss M maintained unhappy with the opinion reached, so the matter was passed to me for a decision.

After reviewing all the evidence provided by both parties, I issued a provisional decision on 22 November 2022. This set out the following:

'Jurisdiction

While our Investigator has addressed the merits of this complaint, and CO hasn't raised jurisdiction as an issue here, there are elements to this complaint that I feel appropriate to cover before discussing the merits of it.

CO has told our service that it doesn't believe Miss M is the genuine applicant of the credit card subject to this complaint. If our service were to agree with CO, then we wouldn't be able to look into this complaint. Broadly, that's because Miss M wouldn't be a customer or potential customer of CO. She would also not hold one of the relevant relationships required between a customer and a regulated financial business: as set out in the Financial Conduct Authority's Handbook (DISP).

Having reviewed the evidence subject to this complaint, I see no reasons to believe Miss M didn't make the application. In summary:

- *The personal information provided in the application matches that provided to*

our service.

- *Miss M has further confirmed this by providing a photograph with her holding her genuine identification: again, matching that provided to CO.*
- *When CO sent Miss M a letter to her home address asking her to get in touch, as it had doubts around the credit card application, Miss M called, confirmed she was not a victim of impersonation, that she'd made the application and provided supporting evidence.*
- *CO has also presented a telephone call to our service that it deems to be suspicious as it thinks another person was making it. Having listened to the call, and on comparing it with other calls CO has provided, and those with our service, I'm not persuaded it has reached a reasonable conclusion.*

CO also appear to acknowledge some of these facts in numerous correspondences with both Miss M and our service but has at times maintained that it doesn't believe Miss M was the genuine applicant.

So, for clarity, I'm persuaded that Miss M was the genuine applicant, and therefore that our service can look into her complaint.

Application of fraud markers

CO decided to load fraud markers against Miss M's name regarding the application utilising a number of fraud prevention databases.

One of the markers—loaded to the Cifas database—was loaded as a victim of impersonation marker. This marker is designed to protect consumers that have fallen victim to identity fraud and alert other members to the details used in fraudulent applications.

Here, Miss M hasn't been impersonated. She has admitted to making the application, using her own details and without any malintent. Therefore, there was no need for the victim of impersonation marker to be loaded against her name. It had no value in protecting Miss M or alerting other members to the information used.

CO has presented evidence to our service that relates to separate applications in third-party names and a potential risk to Miss M's information security. But that isn't why it loaded the marker initially. And I also don't find it fair or reasonable that it maintains the marker on the basis of a potential risk where the marker specifically relates to a victim of impersonation.

Miss M has also provided our service with evidence that CO loaded a fraud marker against her name using the Synetics Solutions database, and has provided testimony that there is a further marker registered with National Hunter: both of which are fraud prevention databases.

For the same reasons I've provided above, I find any adverse marker that has been placed against Miss M's name that is visible to third-party businesses to be unfair in the circumstances.

It's clear that Miss M has applied for the credit card subject to this complaint and therefore CO had no reasonable basis to have recorded any fraud markers against her name. There is also no evidence to support Miss M provided any falsified information of evidence to support her application.

What CO should do to put things right

For all the reasons I've given above, CO should now go ahead and remove all fraud markers it has recorded against any database that are visible to third-party businesses and members, without delay.

I don't find CO has acted fairly here. It has admitted to loading the markers prior to giving Miss M a chance to respond to letters it sent highlighting its concerns. And I don't find, from the information provided so far, that CO had sufficient concerns to load a number of adverse markers against Miss M's name.

While I realise the victim of impersonation marker is generally utilised to protect consumers, it wasn't necessary here. And this would have caused Miss M unnecessary inconvenience in extended security and identification processes.

It also contradicts the additional markers recorded against Miss M's name where it appears to have treated her as a suspect in fraudulent activity. This caused Miss M's accounts to close with third-party banks and denied her access to services such as a communications contract.

Miss M has also disclosed that she has suffered distress as a result of the marker. Understandably, she has expressed confusion and dismay at why this has even happened in the first place considering she was merely applying for a credit card and has now been accused of committing fraud and being impersonated.

This has clearly impacted Miss M and I find that £500 is a fair and reasonable payment to compensate Miss M for impact caused.'

Both parties were provided until 6 December 2022 to respond with any further points before a final deision was made. As both parties have now responded prior to the deadline, I'm now in a position to reach 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.

Both parties have responded to my provisional findings stating that they agree with them and have no further points to add.

Therefore, I don't intend to depart from the provisional findings reached. There are also no further points to address.

My final decision

For the reasons I've given above, I uphold this complaint and direct Capital One (Europe) plc to:

- Remove all fraud markers it has placed against Miss M's name that are visible to third-party businesses and members.
- Pay Miss M £500 in compensation for the distress and inconvenience caused.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss M to accept or reject my decision before 30 December 2022.

Stephen Westlake

Ombudsman