

The complaint

Mr S complains he had to provide a copy of his driving license when opening a new Collection Pot with Modular FS Limited (MFS). He complains MFS collected additional sensitive information that wasn't necessary.

What happened

The details of this complaint are well known by both parties, so I do not intend to repeat the issues in detail here, but in summary:

Mr S explained he organised a Collection Pot through MFS for a leaving collection. Mr S said he collected about £500 in this Collection Pot for a colleague, explaining he wouldn't benefit from this collection himself.

Mr S said MFS requested further personal information, including identification documents. Mr S explained as he wasn't going to be the beneficiary of the account he was unhappy MFS had collected information such as his nationality and date of birth from his driving license. Mr S said MFS explained it was completing due diligence checks, but Mr S said he had looked into this and didn't agree he had reached the threshold for these checks.

Mr S explained he was concerned about a breach of MFS data occurring in the future. He explained the information MFS held about him could be used for fraud and would be damaging to him if it was. He explained MFS had a full copy of his driving license on file, which he argued it didn't need. Mr S said he had used the Collection Pot service three or four times before and hadn't needed to provide his identification.

Mr S said he wasn't disputing MFS needed to undertake due diligence, he was complaining it had collected more information than it needed to when he provided a full copy of his driving license. He also said he wouldn't object to *'individual's screening'* if he had been the beneficiary.

MFS explained Collection Pot is a regulated activity and therefore subject to various legal obligations, including complying with the Money Laundering Regulations 2017. MFS explained it is required to undertake due diligence measures to mitigate the risk of money laundering. MFS said it complied with these regulations by collecting a copy of Mr S's driving license and a short video for biometric purposes. MFS said this was part of its terms and conditions when opening an account. It also confirmed it hadn't suffered any data breaches.

Our investigator didn't think MFS needed to take any action. They explained Mr S had entered a business relationship with MFS and it had therefore correctly asked for identity documentation to complete due diligence. They didn't think it was unreasonable for MFS to retain a copy of Mr S's driving license.

Our investigator also explained if a data breach occurred then our service would be able to investigate the impact of this, but explained we are not a regulator and can't check a business's security processes or compel a business to change such practises. They also explained we can't consider compensation for hypothetical scenarios or what might happen in the future.

Mr S disagreed with our investigator's recommendation explaining he remained of the view MFS had collected more of his personal data than was necessary. Mr S reiterated concerns about data breaches and said he expected businesses to reduce the amount of sensitive

data they hold. He explained such an approach would lessen any damage a potential data breaches may cause to customers.

As Mr S disagreed with our investigator's recommendation, his complaint has been passed to me to make 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.

I appreciate how strongly Mr S feels about his complaint. Although I may not mention every point raised, I have considered everything but limited my findings to the areas which impact the outcome of the case. No discourtesy is intended by this, it just reflects the informal nature of our service.

Where evidence is incomplete, inconclusive or contradictory, I have to make decisions on the balance of probabilities – that is, what I consider is more likely than not to have happened in light of the available evidence and the wider surrounding circumstances.

It may help if I first explain the limitations of our service when considering this complaint. The Financial Ombudsman Service doesn't have the power to fine companies or change businesses process or procedures, we can only consider whether the customer was treated fairly and reasonably in the circumstances of each individual case. We consider what happened, whether the business made a mistake and/or treated the customer unfairly or unreasonably, and if so, the impact this had on the consumer. We then consider what resolves the issues fairly and reasonably for all parties considering all the circumstances.

Financial businesses are under wide ranging and extensive legal obligations to detect and prevent different types of crime and are obliged to monitor business relationships with customers. This is often referred to as customer due diligence or know your customer (KYC). Mr S appears to be aware of these obligations as he has cited some of the legislation in his response to our investigator's recommendation. I can also see MFS provided details of the legislation in its final response to Mr S.

Briefly, these obligations mean businesses must ensure they have current information about their customers which it can use to identify a range of illegal activities. It can also use this information to detect and protect customers from fraud. Failure to comply with some of these requirements can, and sometimes does, result in severe financial penalties for businesses.

Firstly, I agree with our investigator that, regardless of the ultimate intended recipient of the Collection Pot, Mr S was in control of these funds for a period of time. Thus I am satisfied he would have met the definition of a customer in a '*business relationship*' for due diligence purposes.

I now move on to the necessity and details required for compliance with KYC. The legislation and the checks and questions businesses can ask isn't prescriptive. Businesses therefore have latitude to put in place their own policies and processes around this legislation and build their own systems taking into account their own appetite for risk.

For me to uphold this complaint, I would need to be persuaded MFS had acted unfairly or unreasonably when asking for and retaining the information in question.

Asking for identity documents such as driving licenses isn't an unusual practise, indeed I would expect businesses to require some form of approved identification before opening a new financial product, which I accept could include '*special category data*'. As I have said, the obligation on businesses to maintain and keep such information is ongoing, in summary, it is a requirement for them to obtain this information and accurately maintain records of their customers personal details.

I would like to assure Mr S I do appreciate the arguments he has made regarding whether MFS has obtained more information than it strictly needs. Mr S has said he considers his date of birth, nationality and his signature as examples of this excessive information citing this a special category data.

I have considered carefully whether I think this is unreasonable and have balanced this with the wider legal requirements on MFS. I'm also mindful of the limitations of our service when examining this matter.

I don't think the information gathered is more intrusive or excessive than I would reasonably expect. The details gathered are regarding Mr S's personal identity and don't appear to have strayed outside of this information. I am also aware many other financial institutions, particularly online based businesses, gather similar information. It is certainly not unusual in my experience for businesses to keep scans or copies of identity documents on their systems whilst the person remains a customer.

I am also aware Mr S cited several statistics in his correspondence regarding fraud and data breaches. The checks mandated by KYC and money laundering legislation is to assist with the detection and prevention of such offences and to help businesses ensure such losses are mitigated against.

For these reasons, I am not persuaded MFS did anything wrong by either requesting a copy of Mr S's driving license or keeping it on file.

Finally, as I alluded to, some of the issues Mr S has raised are matters beyond the remit of this service, such as internal data security processes. I was pleased to see MFS confirmed it hasn't had a data breach; I therefore will not consider this matter further as it is speculative. Such data handling issues may be matters for the regulator, the Financial Conduct Authority (FCA), or the Information Commissioner's Office (ICO).

I appreciate Mr S will likely disagree with my decision, but I trust I have explained in sufficient detail why I am not persuaded MFS has done anything wrong.

My final decision

For the reasons I have given my final decision is I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr S to accept or reject my decision before 20 August 2025.

Gareth Jones
Ombudsman