DRN-2322355

The complaint

Mr B was a customer of MYJAR and had been since 2016. He complains that he was sent a file containing his personal details when he had not requested it.

A second issue related to a 14 June 2020 email request from Mr B to MYJAR to ask about a debt collection agency and outstanding balance following a default on one of the payday loans Mr B had with it. Mr B says that he never got a reply to that 14 June 2020 email about this.

What happened

Mr B says he never requested the file of personal information to be sent to him by email, or at all. Mr B says he has not been able to access his on-line account in order to make that request. Mr B says that the knowledge and information that he has received in the email 'zip' file plus the password to access that 'zip' file was in his email in-box and led him to feel nervous about having it there, and available to anyone including an email hacker. He blames MYJAR for sending it to him and making him feel that way.

MYJAR says it sent the information to Mr B and it was in response to a data subject access request (DSAR) under the General Data Protection Regulations (GDPR). MYJAR's Head of Information Technology (IT) has investigated and has informed MYJAR of what he has found. MYJAR has explained to me that

'*…a DSAR can only be activated on the client end, by the client logging in and completing an online form. This can in no way be done internally by anyone.'*

MYJAR has explained that the on-line access is particular to the customer and in this case Mr B would have created that on-line access when he first became a customer. MYJAR has sent me a record to show that on 17 April 2016 Mr B did do that. MYJAR's Head of IT explained to me:

'…the internal system is designed to capture only the first login IP address for the client when they create their account as this is used as part of our KYC checks which confirm their IP address is within the geographical location of the residency address for said application.'

I have been sent screenshots of that initial set-up. 'KYC' refers to 'know your customer' and usually relates to new customers and verification checks.

MYJAR says that Mr B did request the DSAR; that it sent a confirmation email to say that he had requested it giving him a time frame when it would arrive; that the DSAR information was sent to him securely and he only complained after he had tried to open it. The outcome from the MYJAR internal investigation is that this request could not have come from anywhere else other than Mr B.

MYJAR has said it is satisfied that Mr B's data has been handled in accordance with regulations and guidance from the Information Commissioner's Office (ICO), GDPR and Financial Conduct Authority (FCA), and the data has not been exposed without his consent.

One of our adjudicators looked at all of this and came to an opinion that MYJAR would have had no reason to think that the DSAR request was mistakenly asked for. Our adjudicator thought that it was reasonable for MYJAR to have treated this as a genuine request.

Our adjudicator had reviewed the copy correspondence MYJAR sent to us. It showed that the MYJAR DSAR team initially emailed Mr B on the 23 June 2020 to confirm receipt of the request and then emailed the DSAR information to him on the 13 July 2020 to Mr B. Mr B's objection to the DSAR was dated 14 July 2020 which post-dated MYJAR having sent the information to Mr B.

Mr B has been asked for any email correspondence he may have sent to show that between the alleged request and the receipt of the DSAR material he queried the DSAR request and/or was objecting to it. He has not supplied that. There may not have been any to show us. MYJAR says it has searched for correspondence and it does not have any such emails.

Our adjudicator looked at the method of conveying the information to Mr B, and she thought that MYJAR had followed GDPR Guidance and had sent it using an encrypted 'zip' file and each document was password protected. The password details were sent to Mr B under separate cover. So, she did not think that this had been sent insecurely.

On the debt collection and balance query of 14 June 2020, our adjudicator had seen the email to Mr B in which MYJAR had responded to that query on 18 June 2020. She explained this to Mr B in her letter of opinion.

Mr B replied to our adjudicator and did not need to know more, or make further points, about the 14 June 2020 query, and so I take it that this element was resolved.

On the DSAR part of his complaint, Mr B made a simple point which is that he has not been able to access his on-line account and so he says he could not have made the DSAR request. He maintains that MYJAR got it wrong.

He has not explained what loss he has suffered due to this error. So, it seems that Mr B is claiming distress and inconvenience for the mistake.

The complaint remained unresolved and was passed to me for a 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.

The GDPR is the legislation that protects how people's data is used and gives more rights and control over how organisations use their data. It replaces the Data Protection Act 1998. It's not our role to decide if a business has breached data protection laws. This is for the Information Commissioner's Office (ICO) to decide. Mr B will have to refer his concern to that office of the ICO if he wishes this to be decided upon.

But I can consider whether it's fair and reasonable to tell MYJAR to pay compensation or take any other action to recognise the impact of what's happened to Mr B.

Since Mr B requested that I review the complaint, I have asked MYJAR again to look into the systems and to see if it can discover whether Mr B was able to access his account on-line, and the origins of the DSAR request once again. Its response has been prompt and the conclusion is much the same as before. This is succinctly explained in this paragraph from

the first set of submissions to this service from MYJAR (the customer number has been removed for privacy reasons):

'Having reviewed the automated email sent to our DSAR team, the Customer ID matches to the customers account with MYJAR (****) and the "Quick Link" is an internal link generated to the customers account within our relationship management system, therefore we are in no doubt that this request originated from the customers online account area'.

And I have already set out the recent Head of IT's response to these queries and these are in the 'what happened' section of this decision.

I asked MYJAR specifically about Mr B's concern that he has not been able to log-in to his account area. MYJAR has said that it does have system limitations and it is not able to provide me, or Mr B, with specific login dates and times, which is unfortunate. But it did explain that

- Mr B had created his account when he first registered to access the website application process and it has produced evidence of that; and
- a system error generated DSAR request would have led to there being a mis-match in information which there was not in Mr B's case; and
- if a third party had requested the DSAR then it would have meant that the third party had access to Mr B's email address, secure password and his MYJAR PIN. MYJAR has described this as '*unlikely*'; and
- Mr B and MYJAR have provided evidence about events which occurred on the same day – 14 June 2020. Mr B emailed MYJAR about the debt and MYJAR has shown me evidence of the auto-generated internal instruction email precipitated by the DSAR on-line request on the same day and within a short time of each other.

Having read all the evidence and considered all the points by both MYJAR and Mr B then I have decided I am satisfied that – on the balance of probability – Mr B likely made that request.

I have tried to establish the on-line access point records Mr B has stressed as being a vital point for him. MYJAR can't send me more than it has, and it is not for this service to delve into the internal workings of a company's on-line system for clear proof. This is an informal dispute resolution service and on the evidence I have, I think it's more likely than not Mr B generated an instruction to the DSAR team and asked for that DSAR.

I have looked for evidence, no matter how slim, to see how and when Mr B may have accessed or used the MYJAR website and/or his on-line account area before June 2020. I am satisfied that Mr B created some sort of MYJAR account when applying for a loan in 2016 and I have seen records of that registering with the MYJAR systems. So, I do think it's likely that Mr B did have some sort of MYJAR account accessed on-line.

In addition, MYJAR has told me that Mr B had asked for a DSAR before. In relation to that earlier DSAR request by Mr B, MYJAR has commented that he did not raise any concern about the method of it being sent to him then. And so, if this is correct, then I think its likely Mr B did have access to the on-line account area to make that request; and/or had no issues then about it being emailed to him. So, I have no reason to think Mr B did not have access in 2020. And I do note that Mr B has not been clear as to whether he has never had access to the on-line account part of the website or whether it was just for the period around June 2020.

My view is that it is for the ICO to assess whether MYJAR's method of sending the DSAR information to Mr B or to any other customer was unsecure. Compliance with GDPR

guidance and regulations is not an area that this service looks into. But I have looked at the impact on Mr B to assess whether I think that he has suffered any distress or inconvenience by the DSAR information being sent to him in the way that it was. And I do not think that it has.

Mr B has explained that he had feelings of concern and nervousness about all the private information being in his email in-box, and therefore potentially being exposed to an unknown and unidentified email hacker. I think that this concern is based on conjecture as to what might have happened. Mr B has not gone on to say that his emails *have* been hacked – and even if he had and his emails had been accessed by an unauthorised third party it would not be something I would consider reasonable to attribute to MYJAR.

I do not think it was unreasonable for MYJAR to treat the DSAR request as a genuine request and act on it in the way that it did.

I cannot take this any further. My final decision is that I do not uphold Mr B's complaint. It's for Mr B to accept my decision or reject it. If he chooses to reject it then he is not bound by it. And in any event, Mr B is free to refer any issues he may have about GDPR to the ICO.

My final decision

My final decision is that I do not uphold Mr B's complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr B to accept or reject my decision before 8 January 2021.

Rachael Williams
Ombudsman