DRN-5352619

The complaint

Miss M complains Eastwood Financial Solutions Ltd ("EFS") was responsible for a security breach by virtue of which fraudsters accessed personal data and funds from an ISA she held on a third-party platform.

Funds were transferred from the ISA to a new bank account the fraudsters set up using a passport scan Miss Ms says was obtained from EFS.

Miss M says neither EFS nor the ISA platform provider will take responsibility for causing the breach. She seeks compensation for the distress she suffered and for harm that might arise in future from the breach and loss of security to her personal data.

Miss M is represented by a relative but for simplicity I've referred throughout to Miss M when referring to things said or done by Miss M or by her representative on her behalf.

What happened

Miss M's online ISA account was accessed by fraudsters who linked new bank details to the ISA. The bank account linked to Miss M's ISA in this way was an account in Miss M's name set up by the fraudsters. Withdrawals were made to the new bank account from the ISA on 14 September, 27 September and 4 October 2023. In total £17,500 was taken.

As a result of the breach and fraudulent access to Miss M's account, the fraudsters also obtained access to sensitive personal data of Miss M and financial records relating to her.

The ISA platform sends emails to customers when certain account transactions take place. Miss M was accordingly sent notification when the new bank account details were added. But she did not pick up on these – in part because of the volume of 'spam' emails she says she is used to receiving.

When the fraud was picked up, EFS alerted the platform provider who on 16 October 2023 decided to reimburse Miss M's account in full for the withdrawals as a gesture of goodwill.

Our investigator thought the complaint should be upheld and proposed that EFS pay redress to Miss M of £800 for distress and inconvenience arising from this matter. Our investigator also suggested EFS pay in advance for the cost of a data security service at £14.99 a month for five years, and refund Miss M what she'd paid to replace her passport, with interest on top from the date she paid this sum.

EFS didn't agree it was at fault, but it agreed to pay our proposed award in the interests of settling matters for all partes. Miss M said being taken seriously was an important step for her in recovery as a victim of this matter, but she said the proposed award didn't match the real and lasting effect the matter had had on her. EFS considers our award was excessive. It still rejects our investigator's conclusions, but it has agreed not to contest liability and asks instead that I consider its submissions on redress.

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.

EFS emphasises this matter is complex and says it is very difficult for definitive findings to be made on liability – that is to say, whether the details used to access Miss M's account were obtained by the fraudsters from EFS. But even if those details did come from EFS, it doesn't necessarily follow that this was the result of negligence. The absence of activity records dating back to the likely time of the breach, means that if EFS's systems were accessed it is unclear exactly how. As such, while I reach my conclusions on the balance of probabilities, there is necessarily a degree of uncertainty as to whether it was a fault by EFS that enabled access or whether access was gained by means that would've succeeded regardless.

However, I don't need to reach a firm view on this point here because EFS has said it will not contest the issue of liability. As such I proceed on the basis that it is likely a vulnerability on EFS's part at least contributed to the breach. So I focus here primarily on the impact of the breach on Miss M and on what would be fair redress for EFS to pay for this. I therefore don't need to discuss the detail of or review further the reports that parties produced speculating about how the breach may have occurred.

Our investigator suggested EFS pay Miss M £800 for distress and inconvenience arising from this matter. In reaching that view, she noted our awards are not intended to be punitive – they are intended to reflect the degree of distress or inconvenience suffered.

There is of course no direct relationship between suffering of this sort and financial redress. So financial awards may seem inadequate from one viewpoint but excessive from another. Deciding on the amount is not an exact science. What I must judge is the personal impact – and this will be subjective and vary amongst different individuals in situations that might otherwise be similar. Our website gives some examples of situations we have encountered in the past and awards we have made as a result. But in the end each situation is unique.

Miss M says a fair award would take account of the sensitivity of the data stolen, the ongoing misuse risk, the lasting emotional stress, the impact of the long investigation timeline – as well as her young age and the preventable nature of the breach. She says the scale of the award proposed by our investigator sends the wrong signal to the industry.

But my awards aren't intended to signal to the industry in general – nor are they designed to punish firms. I do not act as industry regulator. My role is to resolve individual complaints fairly. My awards are designed to be fair for the detriment suffered by the complainant in the particular case under consideration.

Miss M emphasises that personal data accessed by the fraudster were details that weren't shared elsewhere and their misuse by fraudsters led to damage to her credit record, related to the bank account the fraudsters established in her name. She says she has spent an extraordinary amount of time and effort trying to repair the situation. She says this includes speaking to banks, taking advice and keeping watch for any further misuse. I note some of this may have been done by her representative on her behalf.

She points out the data accessed included most identifying details like as National Insurance number, date of birth, address and her email address – as well as bank details and details of her financial history. She says this created a long-term risk – she will live with the uncertainty associated with it for years to come. She says she faces as a result additional unnecessary hurdles in future when doing things such as applying for phone contracts, opening bank accounts or obtaining other financial services. She says this, and the concern her data might

be misused again in future, has had a significant emotional toll. She says scam emails and phone calls she receives evidence that details accessed in the fraud remain in circulation. She says this matter has overall had a significant impact on her health.

Miss M says she feels her stress and the fact her identity was stolen didn't seem to matter much to the regulators. She says UK GDPR Article 82 which makes clear that individuals can claim for both financial losses and non-financial harm such as distress, damage to reputation and inconvenience. She says these principles are relevant when deciding what is fair and reasonable – as this is exactly the sort of harm she has suffered. I would mention here that my rules do allow me to award redress for matters such as these – and it is indeed because of such matters that I make an award here.

My purpose in making my award is primarily to reflect the impact of the breach on Miss M. How the breach arose is not directly relevant to that in my view. So what Miss M says about EFS's security standards being poor, isn't something I reach a concluded view on here as it would not provide grounds to increase my award. I take into account that this dispute has been ongoing for some time, but in that specific regard I also take into account that EFS offered to settle the matter by agreeing to our investigator's award when it was first made.

EFS points out testimony about the impact on Miss M has come from her representative rather than from her direct. It notes she is in her mid-twenties, employed with some financial services experience and from a generation that tends to be tech savvy and communicate by email. It says she could've but regrettably didn't act on notification emails from the platform which it says would've stopped the fraud at the start had she alerted EFS to these.

EFS does not dispute that this issue was no doubt distressing, but it says the situation isn't irreversible and should not have a lasting impact on Miss M in the medium to long term.

EFS says the email Miss M would've received telling her that new bank details had been added to her ISA included the following: *"The updated bank account details will be used for any withdrawals from your… ISA… If you have any questions, please contact our customer service team on…. or go to the contact us section [of the website]"*. EFS says no weight appears to have been attached to Miss M's failure to act on the emails.

EFS emphasises that it acted urgently to notify the platform provider as soon as it was made aware of the breach – and it points out it doesn't receive email notification when transactions are carried out on client accounts like Miss M's, so it couldn't have picked up on those in the way Miss M could have. It says it contacted the relevant authorities thereafter and it says it received feedback from its regulator – the FCA – that by commissioning expert reviews it had gone over and above what would be expected in its response.

In summary EFS considers our investigator's redress proposal grossly disproportionate and unfair, taking into account redress paid by or awarded against other parties in this matter and bearing in mind what matters were and were not within EFS's control.

I note all EFS says about the email alerts Miss M was sent. It seems Miss M didn't view the emails as something she needed to pay close attention to, and so she did not question or act on their contents. I agree this is regrettable because had she done so the fraud might not have got as far as it did.
But I don't think it fair to place too much blame or responsibility on Miss M for this. The emails were a potential safeguard, but the security of Miss M's account wasn't supposed to depend on whether or not she responded to email alerts she was sent. She missed an opportunity to stop the consequences of the breach sooner, but she wasn't the source of the breach in the first place. Also – and this is important – acting on the email alerts would have

done nothing to prevent the loss of privacy suffered by her data when her account was accessed - because that access preceded any email alert sent to her about it.

So I do give some weight to the fact Miss M did not react more quickly. I acknowledge this had some consequences. But I don't see that this made a significant contribution to bringing about or worsening the situation that arose for Miss M in this case.

I say this bearing in mind the funds withdrawn from her account were returned to her by the platform, so there was no lasting financial loss from that point of view. Had that not been the case, the question of to what extent Miss M ought to have acted on the emails may have had more significance and required more detailed consideration. But that is not the case here. There is nothing Miss M could have done to prevent the loss of data that forms the major part of the ongoing detriment under consideration here.

I agree with our investigator that the compromise of Miss M's personal data was significant. Fraudsters not only accessed her ISA and linked new bank details to it, they also created a new bank account in her name. It seems to me this would naturally deepen the concern caused to Miss M by the unauthorised access to her ISA - regardless of the source of the passport scan used to create the bank account. So it seems to me on any view it is entirely understandable that the impact on Miss M was significant in terms of distress. I accept that the testimony we have about this impact comes from Miss M's representative rather than from her directly, but I don't see that much turns on that point.

Having thought carefully about all this, I find that the breach did cause Miss M both inconvenience and distress – distress both arising from the breach itself when it occurred and the fear of financial loss, but also from the ongoing inconvenience and concern about the future misuse of the data that was accessed. With this in mind, I view £800 as a fair and reasonable sum for EFL to pay her for distress arising – and for inconvenience from the additional precautions Miss M takes in future as anticipated by her in her submissions.

Miss M says EFS was not cooperative. Insofar as that was so and impacted Miss M, my view is my £800 award reflects this adequately.

The funds taken from Miss M's ISA were reimbursed, so there is no financial loss of that kind for me to consider here. Miss M says EFS didn't provide a basic standard of care, and she suggests a refund of fees in light of this. But in my view the right remedy is an award for her distress and inconvenience. I don't think the breach is evidence that EFS wasn't providing Miss M with a service in return for what she was paying to EFS.

I agree with our investigator that paying for a data security service is appropriate as it helps to mitigate the impact of the breach – and so addresses in part the ongoing concerns Miss M has expressed. Our investigator suggested EFS pay this for five years. Miss M says a period of seven years would be more appropriate. EFS suggests that over the medium to long term the impact of the breach will dissipate. I'm not sure that I agree that the impact will dissipate entirely, but in my view a five year period is fair and reasonable here.

Our investigator also considered that EFS should pay Miss M for what she paid to replace her passport – with interest on that sum from the date she paid for it. I agree EFS should pay for the refund because replacing the passport was a necessary step towards repairing the damage that resulted from the breach in the short-term.

I won't award interest on the refund though because the sum would be trivial and complicate the redress unnecessarily. Also, payment for the data protection service fees in my award is in advance, so ignoring interest on the passport refund seems fair overall in light of that.

So, for the reasons I've given, and to the extent I've explained, I uphold Miss M's complaint.

Before closing I would like to thank the parties for their assistance and for providing prompt and helpful submissions to us throughout the course of our inquiries. I'm grateful to Miss M's representative for the time she has taken in putting together submissions for Miss M.

Putting things right

To put things right, Eastwood Financial Solutions Ltd must:

- Pay Miss M £800 for distress and inconvenience she suffered as a result of the breach.
- Pay Miss M £899.40 (being £14.99 a month towards a subscription to a credit reference agency, paid for five years and paid upfront as a lump sum).
- Reimburse Miss M for what she paid to obtain a new passport.

My final decision

For the reasons I've given, and in light of all I've said above, I uphold Miss M's complaint.

Eastwood Financial Solutions Ltd must put things right by doing what I've said above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss M to accept or reject my decision before 9 September 2025.

Richard Sheridan
Ombudsman