DRN-5970728

The complaint

Mr M complains TransUnion International UK Limited has acted unfairly by allowing unauthorised access to his credit file.

What happened

In July 2025, TransUnion wrote to Mr M telling him his information had been involved in a data breach. This meant some details from his credit file had been accessed by a third-party. It explained this happened between 12 June and 5 July 2025. It set out the information that had been accessed and confirmed it had removed the search from his credit file. In addition, it offered Mr M a 12-month subscription to its TrueIdentity Service.

As Mr M didn't think this resolved matters, he complained, in summary asking TransUnion to:

- Explain the steps taken to remedy the breach
- Whether his data had been misused since the breach was discovered and whether TransUnion had since carried out an audit of access to his credit file
- The name and contact details of its customer who accessed the data
- The compensation it would pay, in addition to TrueIdentity

TransUnion looked into things but didn't think it needed to do anything further. As a result, Mr M referred his complaint to this Service.

An Investigator here reviewed matters and agreed the breach shouldn't have happened. But considered TransUnion acted promptly in addressing it and fairly resolved matters by offering a 12-month subscription to TrueIdentity and removing the soft credit search. They acknowledged the situation was undoubtedly concerning but said there wasn't enough to show ongoing impact to Mr M as a result of the breach.

Our Investigator later explained that TransUnion wasn't responsible for how third parties safeguard their own login credentials. But must respond appropriately when inappropriate use is detected – which it did. They also explained it wasn't this Service's role to decide whether a business had complied with data protection legislation.

Mr M didn't agree and in summary said TransUnion was responsible for the breach that had occurred – which was long lasting and had a significant impact on him. He reiterated it had caused harm, by giving access to his personal details to an unauthorised party and TransUnion hadn't explained what had happened and how. He also said the impact to him wasn't hypothetical, as our Investigator had said. This was because his employment required enhanced security screening, which included details on data breaches and unexplained access to his credit file. As a result, he didn't consider a 12-month subscription to TrueIdentity fairly resolved matters.

As no agreement has been reached this complaint has been passed to me to decide.

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.

In doing so, I've taken into account the relevant industry rules and guidance, and what would be considered as good industry practice.

Firstly, I want to explain I've read and taken into account of all the information provided by both parties, in reaching my decision. If I've not reflected something that's been said it's not because I didn't see it, it's because I didn't deem it relevant to the crux of the complaint. This also means I don't think it's necessary to get an answer, or provide my own answer, to every question raised unless I think it's relevant to the crux of the complaint.

I also wanted to set out the basis on which I'll be deciding this case. The Financial Conduct Authority (FCA) sets out in the Dispute Resolution (DISP) rules the following:

DISP 3.6.1

The Ombudsman will determine a complaint by reference to what is, in his opinion, fair and reasonable in all the circumstances of the case.

DISP 3.6.4

In considering what is fair and reasonable in all the circumstances of the case, the Ombudsman will take into account:

(1) relevant:

(a) law and regulations;

(b) regulators' rules, guidance and standards;

(c) codes of practice; and

(2) (where appropriate) what he considers to have been good industry practice at the relevant time.

The effect of these rules mean I'm required to take into account the information, laws and legislations Mr M has mentioned, but I'm not bound by them. This reflects our informal nature as an alternative to the courts. As such, we wouldn't routinely quote every law that could potentially apply.

I should also explain, this Service is not the regulator, that's the role of the FCA. So while Mr M considers TransUnion should be required to follow certain processes, even if I found that TransUnion had acted unfairly, I wouldn't be able to instruct it to change its processes as a result.

As our Investigator has explained it's not the role of this Service to decide whether TransUnion has complied with the data protection legislations he's referenced – that's the role of the Information Commissioner's Office, which I understand Mr M has already referred his concerns to. I can however consider whether TransUnion has acted fairly in putting things right, as I'll come on to explain.

What happened and how TransUnion put things right

In this case an unauthorised party gained access to some of the information on Mr M's TransUnion credit report. Based on the information I've been provided; it appears it did so by using a third-party business' log in details for its consumer credit checking service – which uses data from TransUnion.

When TransUnion became aware of the breach, it stopped access to prevent the unauthorised party carrying out further searches. It also notified Mr M some of his data had been accessed and removed the soft search from his credit file applied as a result. In addition, TransUnion offered Mr M 12-months access to its TrueIdentity service – which is designed to help customers following a data breach. This seems reasonable and the steps I'd expect TransUnion to have taken, given what happened. I'm also pleased to see it did so promptly after becoming aware there was an issue.

On this point, as our Investigator explained, I don't find TransUnion to be responsible for the unauthorised party accessing this information. That's because they used true log in credentials, so initially there was no realistic way for TransUnion to know an unauthorised party was accessing Mr M's data. As a result, all I'm able to consider is how TransUnion dealt with matters once it became aware there was an issue and any impact caused to Mr M, solely as a result of TransUnion's actions.

I appreciate Mr M considers TransUnion didn't act quickly enough to resolve matters and considers it should have detected the issue sooner. But based on what I've seen, once it was detected, it stopped the access and put in place a resolution promptly.

The impact on Mr M

I can appreciate it would have been extremely distressing for Mr M to find out his details had been involved in a data breach. But by the time he was notified, TransUnion had already worked to resolve the issue and offered him access to its TrueIdentity Service.

Mr M has said, as a result of his employment, data breaches such as this could have significant potential impact on enhanced security clearing he requires. As a result he considers TransUnion's actions have a significant professional risk to him, and he should be compensated for that. Our Investigator said Mr M hadn't evidenced this had caused a direct loss and I agree. While I understand Mr M is concerned this could impact future checks, I can only take into account tangible and identifiable losses. And here, Mr M hasn't shown, since this issue occurred, that he's experienced problems as a result. I also can't ignore Mr M has evidence from TransUnion about the reason this issue happened – which he'd be able to provide to his employer. In the circumstances, I don't think TransUnion could reasonably do more.

In any case, as explained, it wasn't until TransUnion became aware of the issue that I'd expect it to take action to fix it. And until this point I can't agree TransUnion are responsible for the actions of the unauthorised third-party. So any impact they caused, isn't something I can hold TransUnion responsible for.

I should however add, in future if Mr M does find he experiences problems as a result of the issue, and can attribute those to TransUnion's actions, he's able to raise those with TransUnion at that time. But at this stage, it's simply not possible to fairly say TransUnion should award financial compensation when I haven't been able to identify that it's made an error or caused Mr M to suffer such losses.

While I appreciate Mr M also considers its for TransUnion to reassure him his data hasn't

been compromised further, this isn't something I'd expect it to do. I say that because, TransUnion can't know what information, if any, has been accessed or used by the unauthorised party. All it can do is tell Mr M what potential information they had access to – which it's done. As such, I think it's reasonable to give Mr M access to the TrueIdentity Service which helps him to protect his information and be notified of any issues going forward.

And aside from the soft search, which has now been removed from Mr M's credit file, I haven't seen any other incorrect information was shared. As such, I haven't seen incorrect information to have impacted any applications or checks carried out using Mr M's credit file.

Customer Service

Mr M has complained TransUnion hasn't given further details about how the incident happened. I don't think it's unreasonable for it not to share everything with Mr M, such as its internal processes, and it's also not obliged to do so.

That said, from what I've seen TransUnion has shared a large amount of information with Mr M. It told him the parts of his credit file the unauthorised party had access to as well as the business whose log in credentials were used.

Mr M himself has also provided this Service with communications he's had with that business who explained what happened. So it's difficult to know what further information Mr M wants from TransUnion here, that it's reasonably able to provide.

Overall, I think TransUnion has done what I'd expect here. It stopped the unauthorised access as soon as it became aware and notified Mr M about what had happened. It shared details of the information that had been accessed and suggested ways in which Mr M could help protect himself going forward – as well as giving him access to its TrueIdentity service. TransUnion also removed the soft search from Mr M's credit file, as I'd expect.

While I understand Mr M considers he should get financial compensation, I'm required to consider each complaint individually and on its own merits. Overall, as explained, I agree this would have been a stressful time for Mr M, but I've seen nothing to say TransUnion did something wrong or that this has caused financial loss or ongoing detriment. So having considered what happened here, I'm satisfied the 12-month subscription to TrueIdentity fairly resolves matters. I say that because, although it's disappointing this happened, when TransUnion was notified, it worked promptly to resolve the issue and confirmed to Mr M it had done so.

Given this, I won't be asking TransUnion to do anything further.

My final decision

For the reasons explained above, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr M to accept or reject my decision before 19 February 2026.

Victoria Cheyne
Ombudsman