

[View this email in your browser](#)

In order to avoid spam filters, please

[Add us to your address book](#)



20/05/25

LAPG Member Update

Issue 16 of 2025

LAA Data Breach

What do we know so far?

Press release from the LAA

By now you will all be aware of the latest development in the LAA cyber security breach. Official comms from the LAA to providers yesterday explained that on 16 May the Agency became aware that 'the incident was far more extensive than originally understood, with the group behind it also having accessed a large amount of information relating to legal aid applicants'. As a result the LAA has decided to keep 'the LAA Online Portal offline at this time' and invoke a number of contingency arrangements (see below).

We have fielded a large number of understandably concerned emails from members and have been in contact with the LAA to express our concern and seek clarification about some key issues, such as:

- Whether the LAA expects providers to contact all their clients, since 2010, who may have been impacted by the breach? The LAA confirmed last night that they **do not** expect providers to notify clients of the breach.
- What steps the LAA will be taking to notify providers (other than putting a statement online). *We are awaiting an update on this.*
- If the LAA does notify clients directly, will additional guidance be made available to providers on how to respond to the inevitable contact they will receive from distressed clients? *We are awaiting an update on this.* To date,

the LAA has posted on gov.uk that clients impacted should seek guidance on how to protect themselves from the impact of a data breach [on the NCSC website](#).

- How the LAA will deal with processes not covered by the contingency measures outlined in the LAA's comms, such as POAs, HCCs, payments runs. Again, *we are awaiting an update on this*, but the LAA has indicated that clarification will be provided on Thursday.
- Whether firm or individual lawyer data has been stolen and if so, what are the risks and what mitigation should providers take.

We know this is an incredibly worrying time for you all, and we are pressing as hard as we can to get answers from the LAA. We are also in close contact with TLS, LCN and other groups to ensure we understand the full impact on providers and clients.

The Law Society issued this press release yesterday afternoon:

<https://www.lawsociety.org.uk/topics/news-articles/legal-aid-agency-data-breach>

What are your responsibilities as data controllers and processors?

Julie Bishop of Law Centre's Network has sent us the following useful summary following contact between LCN and the ICO:

'Their view is that it is quite likely [legal aid providers] are data controllers with regards to some elements of the legal aid contract, although this may be held jointly with the LAA for certain types of processing – as seems to be the case as listed here: [Data Security Requirements](#)

In other regards, [providers] are also data processors – also indicated in that same document.

Regardless, at this point in time, [providers] do not know precisely what data has been stolen, whether this is high-risk data, and which clients have specifically been affected and to what degree.

[The ICO's] recommendation is NOT to write to all clients at this point in time until we know more information.

There is no requirement to do so at this stage under the ICO regulations, and doing so may have the undesired effect of panicking and worrying clients more than they need to be.

In short, there is nothing much that we can do right now until further details of the impact of the breach are known.

[The ICO's] view is that once the LAA have fully investigated what has happened, to who, what data has been accessed and how the individual is likely to be at risk, they should then notify the legal aid providers to inform them how this breach affects them.

[Providers] should then notify the ICO of the breach with full details of what has happened. Their view is that it is better to log the breach with the ICO and for the ICO to determine that no further action is needed, then to not say anything at all.

They may also then need to notify any clients that have been affected. This would not be possible for any clients that the [provider] saw historically and no longer has records for. But again, you need to wait for further info before proceeding.

In terms of potential repercussions for [providers]:

It would be helpful for [providers] to log the breach in their data registers and any actions they are taking resulting from it, so that they have evidence on how they are handling it, should then need to provide this to the ICO for any reason.

I would also recommend that, regardless, [providers] check that their processing registers are up to date insofar as possible).

The ICO said that it would expect the LAA to be carrying out regular audits of its data processing activities and security measures to ensure they are keeping data safe.

Where a provider is mandating that organisations use a specific portal, the responsibility for the security of that portal rests with the provider – and therefore the weight of any judgement passed would be most likely born by them regarding poor security practices.'

Contingency arrangements

From the LAA update to providers 19.05.2025:

Civil applications:

For civil applications, where a provider cannot utilise delegated functions and has an imminent court hearing they should contact the LAA customer services team on 0300 200 2020.

Crime applications:

Whilst the Portal is unavailable providers will be unable to gain a date stamp for applications. When the Portal becomes available providers will be invited to complete applications as normal and indicate in the 'Further Information' section that they were unable to submit their application and the date that they would have submitted it but for the outage. LAA caseworkers will backdate representation orders to the requested date where applicable.

Crime Lower and Legal Help monthly submissions

Where providers have not yet submitted their April CWA submissions (due by 20 May), they should email the Reconciliation team reconciliation@justice.gov.uk with their total monthly submission value for their April submission by 20 May. This should be a global amount for each submission which the provider normally makes on CWA. When CWA is available, the submissions should then also be submitted via the system, to allow them to be reconciled.

What about the other processes? Members have raised queries about ongoing negotiations on HCCs, submitting POA requests and whether the outage will impact on LAA payment runs. We're aware that some payments expected this week have not landed in provider accounts. We have sought urgent clarification on these issues and hope to be able to provide further information after a meeting we have with the LAA today.

Please get in touch if you have any other questions or concerns.

Take care one and all,

Chris Minnoch, CEO [@ChrisLAPG](#)

Follow LAPG on X [@WeAreLAPG](#) and Bluesky [@wearelapg.bsky.social](#)

#WeAreLegalAid

20/05/25



Subscribe to our courses

Would you like to contribute to our Member Updates and share news and information with other members? If so, just email us and we can discuss how you can best contribute.

Thank you for being brave enough to be part of the LAPG community!



Copyright © 2025 Legal Aid Practitioners Group, All rights reserved.

Want to change how you receive these emails?
You can [update your preferences](#) or [unsubscribe from this list](#).