



Accellion cyber incident – Australian credit licence applicants

Frequently asked questions

What happened and when?

On 28 December 2020, an unidentified threat actor accessed an ASIC server containing attachments to Australian credit licence applications submitted to ASIC between 1 July 2020 and 28 December 2020.

How did the incident occur?

The cyber incident occurred due to a vulnerability in a file transfer appliance (FTA) provided by California-based Accellion and previously used by ASIC to receive attachments to Australian credit licence applications.

When did ASIC become aware of the incident?

On 15 January 2021, Accellion advised ASIC that there has been evidence of unauthorised access to ASIC's Accellion server.

After becoming aware of the vulnerability identified by Accellion, ASIC applied the recommended patch and sought a review of the server access logs from Accellion.

Was any information accessed?

ASIC's initial forensic investigation confirmed there is no evidence that the attachments to the identified credit licence applications have been read or downloaded. This has not changed.

We were of the view in January 2021 that the filenames of attachments for credit licence applications that were submitted to ASIC between 1 July 2020 and 28 December 2020 may have been viewed by the threat actor. For example, the credit licence applicant's name or the name of an individual responsible manager, if these were used in the filename of the attachment (e.g. police check, CV) may have been viewed by the threat actor.

Following additional analysis, it is highly unlikely that the threat actor accessed any data held on ASIC's Accellion server, including the file names of attachments related to Australian credit licence applications.



What has ASIC done to address the cyber incident?

In response to the incident, ASIC has:

- disabled the relevant server;
- ascertained that no other ASIC information technology (IT) infrastructure is impacted;
- provided alternative arrangements for submitting attachments (see below);
- written to all identified credit licence applicants (via the contact email address nominated by the applicant) to advise and update them about the incident;
- assessed the incident in accordance with our obligations under the *Privacy Act 1988*;
- informed relevant authorities; and
- engaged independent cybersecurity experts to complete a forensic investigation.

Are any of ASIC's other data systems impacted?

ASIC's forensic investigators reviewed the evidence and determined that there is no evidence of impact to other ASIC IT systems from the Accellion vulnerability.

Following additional analysis, we now also believe it is highly unlikely that the threat actor accessed any data held on ASIC's Accellion server, including the file names of attachments related to Australian credit licence applications.

Who has ASIC notified about the incident?

ASIC has contacted the credit licence applicants who were initially thought to be impacted (via the contact email address nominated by the applicant) to notify them of the incident. The incident relates only to attachments to applications submitted to ASIC between 1 July 2020 and 28 December 2020. Following additional analysis, we believe it is highly unlikely that any credit licence applicants were impacted by this event.

ASIC has notified relevant authorities, including the Australian Cyber Security Centre. We have been working with Accellion and independent cyber security experts to complete forensic investigations.

What should I do now?

We have all the attachments that credit licence applicants have submitted previously. If ASIC's assessment of these applications is still pending, no further action is required unless you are contacted by ASIC.



How can I contact ASIC about the incident?

ASIC has set up a dedicated email address for all enquiries regarding the incident:
contactus@asic.gov.au

I want to lodge a credit licence application. How do I do that now?

Application forms

The method of submitting ASIC credit licence applications (via ASIC forms CL01 and CL03) has not changed. Applicants are still to complete and submit an application via <https://www.edge.asic.gov.au/011/acrportal/get/ServicesLogin>

Attachments

We have disabled ASIC's Accellion file transfer application server previously used to submit attachments with credit licence applications.

Going forward, when credit licence applicants submit CL01 or CL03 application forms, please contact us at licensing.credit@asic.gov.au. We will then provide details on how to securely submit the accompanying attachments. We have updated our [forms and procedures](#) to set out these alternative arrangements.