



Companies House

Companies House
Crown Way
Cardiff CF14 3UZ

Andy King
Chief Executive and Registrar of
Companies for England and Wales
aking1@companieshouse.gov.uk

Rt Hon. Liam Byrne MP
Chair of the Business and Trade Committee
House of Commons
London
SW1A 0AA

Date: 19 March 2026

Subject: Fault in Companies House's online filing service

Dear Rt Hon. Liam Byrne,

Thank you for your letter dated 16 March 2026 concerning a reported issue with the Companies House WebFiling service. This is a matter I am taking very seriously.

Following confirmation of the issue, I can confirm that we acted swiftly to suspend, fix and then reopen the WebFiling service, which has been operating normally since 9am on Monday 16 March. We issued a public statement setting out the nature of the issue on Monday and have written to all companies, via their registered email address, to clarify the nature of the issue and provide advice. We have also published this on our website and other channels.

It is important to highlight that this is not a cyber attack and there is no risk of bulk data exfiltration. Following the initial report, ongoing investigations have found no confirmed evidence that any records have been changed as a result of this issue. While this is welcome news, I very much appreciate the opportunity to address the Committee's specific concerns while investigations continue:

1. How long was the vulnerability present, and did Companies House only become aware of it after being contacted by Tax Policy Associates?

The issue arose in connection with a major system update deployed on 11 October 2025. The defect could only have been exploited by an authenticated user carrying out a specific sequence of actions, between 11 October 2025 and 13 March 2026.

Our incident monitoring systems are designed to detect system failures and our wider security controls are designed to defend against cyber attacks. As this issue stemmed from a functional defect those monitoring controls were not triggered. We became aware of the issue following an email from a third party on 13 March 2026. We continue to investigate the matter, but we have found no confirmed case to indicate it was exploited.

In recent years Companies House has considerably strengthened its security posture. We operate an ISO 27001:2022 certified Information Security Management System, demonstrating our commitment to rigorous, independently audited security controls. Our approach aligns with recognised government (GovS 007) and industry



Companies House

standards, including the Cabinet Office Departmental Security Health Check and PCI DSS for payment data.

2. Can Companies House determine which company dashboards were accessed during the period of vulnerability?

It is not currently possible to determine the number of times a registered user accessed information by means of the defect, but our ongoing investigations have yet to identify a confirmed instance of a record being inappropriately changed.

Although the defect opened a technical route for registered users to submit changes to individual company records for which they had no permissions, all changes are recorded and linked to that logged in account. This provides us with the ability to trace who changed a company record. At the same time, it means companies can see in the public register if their filing history contains anything unexpected. We continue to assess whether it is possible to provide a comprehensive record to identify those who have accessed data through the technical defect.

3. During this period, were unauthorised third-parties able to make permanent changes to company information?

If a user were able to exploit the defect, they would not have been able to remove or edit an existing file – they remain on the company record – but would have been able to add new filings. Those changes, if accepted, would be visible to everyone in the filing history on the public register.

As a precaution, we have written to all companies, via their registered email address, asking them to check their records to assess if they have any evidence of any inappropriate changes. We have published a copy of this correspondence on our website.

At the same time, we are undertaking extensive analysis of system records to identify any anomalous activity. This has yet to identify any unauthorised changes, but investigations are ongoing. Should we identify any unauthorised changes, we will work with customers to rectify their record and take firm action with the user who made the filing.

4. What support has been provided to potentially affected directors and companies?

We issued a statement on Monday morning (16 March) shortly after reopening the WebFiling Service at 9am and have emailed all companies, via their registered email address, to clarify the specifics of the issue, and signpost actions and next steps for any customer who is concerned. We have also published this guidance across our channels. A copy of both communications are enclosed for reference.

In addition, our customer contact centre, customer care teams and complaints team are on hand to support customers. Customer contact is being closely monitored and continues to operate within normal levels, indeed, by mid-week, overall levels of customer contact were lower than the previous week. We recognise that many



Companies House

companies rely on professional providers and have offered briefings to these providers to enable them to better support their customers.

Finally, we continue to recommend customers to sign up to our free “Follow” service. Follow sends customers an instant email alert whenever a document is filed with us for any company they choose to follow — including their own. It is a simple way for customers to stay informed and spot anything unexpected as soon as it happens.

5. What internal security controls failed, permitting access to private dashboards without authentication reverification?

We continue to investigate the circumstances that led to this issue. Indicative findings suggest that the issue was caused by an application defect which was not identified during testing or by peer review.

6. Have you made any assessment of whether a similar vulnerability may have been created on previous occasions, such as previous updates to the WebFiling system?

The WebFiling service defect was linked to a major service release with a particular profile unlike any other recent service changes. We consider that there is a minimal risk of the same or equivalent issue being associated with other WebFiling service changes. Nonetheless, we are reviewing the situation in detail to derive wider learning.

7. When will the WebFiling service go live again? And will Companies House provide any further public updates about the incident and your response to it?

After comprehensive testing the service was reopened to external users at 9am on 16 March.

8. What measures are being implemented to prevent similar incidents?

In addition to the rigorous testing prior to reopening the service on 16 March, we are taking further actions to strengthen our services. These include a detailed review (lessons learned) of how the WebFiling defect occurred and what processes need to improve as a result. This is supported by recent changes to strengthen our governance and assurance of change overall.

More widely, although this was not a cyber-attack, we are continuing to strengthen our security posture in response to a more challenging threat environment, investing in our security operations centre and other capabilities to mitigate these risks.



Companies House

For the longer term, we are developing a case for investment to modernise our architecture and reduce risks associated with legacy applications. This work is an important part of our plan to prevent economic crime entering the system, protecting companies and citizens from harm, and to extend the value of the information within our registers as a key enabler of growth.

Yours sincerely

Andy King

Chief Executive and Registrar of Companies

aking1@companieshouse.gov.uk