#together

Andy King
Chief Executive Officer and Registrar of
Companies for England and Wales
Companies House
Crown Way
Cardiff
CF14 3UZ

via email

Friday 7 November 2025

Dear Andy,

Thank you for your letter regarding our campaign and the strong public reaction on social media and via emails about the issue of Company Directors and digital ID.

We appreciate the opportunity to engage with your explanation of the policy. You state:

> *"The requirement to provide identity verification will not create a digital ID for company directors.... Rather, it is designed solely to prove that new and existing directors are who they say they are. We will confirm directors' identities using their existing forms of identification, such as a passport or driving licence, and this can be done via the free GOV.UK One Login service or customers can choose to use someone registered as an Authorised Corporate Service Provider such as an accountant."*

We would like to raise several concerns.

1. One Login amounts to a de facto digital ID.

Requiring directors to verify their identity via GOV.UK One Login, uploading a passport or driving licence, and receiving a persistent code linking them to their company record constitutes, in practical terms, a state-controlled digital ID. The assertion that this "will not create a digital ID" glosses over the reality of a verified digital identity link.

This situation is made worse by the Government's shifting definition of what constitutes a "digital ID." Ministers have on the one hand presented digital ID as merely a convenience measure, yet on the other suggested potential expansion into all sorts of concerning areas, including benefits, tax - even apparently "accessing your own money." In effect, One Login arguably already functions as the foundation of a national digital identity framework, introduced before any meaningful consultation on a "card" or other formal identifier. The Prime Minister has repeatedly stated that digital ID will be compulsory *to work,* rendering the notion of "consultation" meaningless and demonstrating that an outcome never mentioned in his party's election manifesto appears pre-determined.

Recent experience has shown how quickly such systems can expand in scope: in the Covid era, digital ID credentials were imposed or proposed for access to venues, workplaces, and public services. 40,000 experienced care workers were forced from their jobs, and a further 100,000 NHS workers threatened under mandatory health policies, with the enforcement mechanism envisaged as a form of state-controlled digital ID ("Covid pass"). Once a system of centralised digital control is created, the temptation to widen its use is overwhelming, with profound consequences for liberty and privacy.

2. One Login appears to pose major security risks, potentially exposing millions of directors' sensitive data if this goes ahead.

From the catastrophic Afghan data breach that endangered the lives of service personnel as well as costing the taxpayer up to £7bn, to the Electoral Commission having 40m voter records compromised, bluntly, the public has every reason not to trust the state with our sensitive data.

It is all the more incredible, therefore, that millions of directors face being forcibly enrolled into the One Login system, despite the serious security failings now widely reported in the media.

In his letter to the National Audit Office dated 21 October, David Davis MP points out the following:

> *"As early as 2022, the information assurance team - responsible for ensuring the security of the One Login system - raised a number of issues (including) the fact that the system was being developed on unsecured workstations by contractors without the required security clearance in Romania…*
>
> *In March of this year, a 'red team' exercise was conducted, with contractors tasked with stress-testing the One Login system. The platform's security was an abject failure, with the read team using an unsecured laptop to gain control of the One Login codebase… (this went) entirely undetected and - if it had been real-world hackers - they could have easily buried their own malicious code in the One Login system.*
>
> ***It is entirely possible that a malicious actor - whether that be a foreign state, a ransomware criminal, or even just a malevolent hacker - could have already compromised One Login without our knowledge, and we may already have malware in the system."***

In all this time, the Government appears to have provided no evidence to refute these serious allegations.

If Companies House persists in compelling directors to enrol in One Login despite clear and reasoned objections, it will do so in full knowledge of the risks. Should the system later be

compromised (or indeed is found to be compromised already), it will be a matter of public record that these risks were expressly raised and disregarded. At that point, questions of legal and administrative responsibility would be unavoidable.

We understand that, under the UK GDPR and Data Protection Act 2018, Companies House would remain a data controller for any personal information it collects through this process, even if it relies on a platform operated by the Cabinet Office. Both bodies would therefore carry joint responsibility for ensuring compliance with Article 32 - including the duty to implement "appropriate technical and organisational measures" to safeguard personal data. Failure to do so would constitute a breach of statutory duty.

Any serious incident would inevitably trigger investigation by the Information Commissioner's Office, which has the power to impose fines, enforcement notices, and public reprimands. But the consequences would not end there. Forcing millions of directors into a system whose security, proportionality, and accessibility have been repeatedly questioned could, in hindsight, appear less as administrative oversight and more as reckless disregard for foreseeable harm. That is the threshold at which regulatory failure becomes a matter of negligence, misfeasance, and political accountability.

3. Forcing directors to use One Login is exclusionary and unjustified.

A study for the Department for Education[1] found that 7.5 million people, or 18% of UK adults, lacked the essential digital skills that are needed for the workplace; other estimates place the number who lack basic digital skills as high as 11m.

Given company directors tend to skew older than the general population, a significant number are likely among those digitally excluded and may struggle to use One Login. Directors who cannot - or do not wish to - use One Login may be forced to rely on an Authorised Corporate Service Provider (ACSP) if they wish to comply, creating unnecessary costs and administrative burdens. This disproportionately impacts those already digitally excluded, including older and disabled directors, effectively penalising the very people who are least able to adapt.

4. Please clarify that the ACSP "route" produces a code usable only by Companies House.

With large numbers of directors having reasonable, rational and serious concerns about One Login, based on our research, we understand the ACSP "route" works differently; namely, it verifies a director's identity with Companies House by generating a code that is only valid for Companies House:

- It is not part of the One Login system
- It is not usable by other government departments

[1] https://commonslibrary.parliament.uk/research-briefings/cdp-2024-0073/

- For many directors, this makes it far less concerning

Please could you make it explicit that if directors register via the ACSP route:

Companies House does not intend - now or in the future - to share this data or information with other government departments, and how the data is to be used.

5. An offline alternative, that doesn't penalise directors, is essential.

A free, non-digital alternative should be made available - and publicised - urgently to ensure directors are not compelled into One Login against their better judgment or forced to incur extra costs.

In the absence of a free offline alternative, given the very serious concerns raised, directors would have legitimate grounds to refuse compliance.

At Together, we advocate for technology that enhances efficiency while safeguarding privacy and choice.

These concerns span a wide range of issues: from the de-banking scandal, to social media censorship, to the Department for Work and Pensions accessing personal bank accounts, to the growing use of biometric verification in everyday life without consent, and to those who simply cannot or do not wish to log in. Millions of pensioners and many others are key examples of people affected by these policies.

We urge that any processes and proposals fully respect privacy, consent, and choice, so that technology serves people - not the other way around.

Thank you, and we look forward to your response.

Alan Miller.

Co-Founder,
Together Association.

Companies House

Date
28 October 2025

Sent by email
Executive Board
#Together

Dear members of the #Together Executive Board,

We have noticed your recent social media activity on our plans to require company directors to verify their identities with Companies House.

I appreciate the interest your organisation and its members have shown in this matter, and I recognise the strength of feeling that has been expressed in the social media we have seen and the emails we have received.

I would like to take this opportunity to clarify the purpose and effect of this policy. The requirement to provide identity verification will not create a digital ID for company directors as has been suggested in some of your materials. Rather, it is designed solely to prove that new and existing directors are who they say they are. We will confirm directors' identities using their existing forms of identification, such as a passport or driving licence, and this can be done via the free GOV.UK One Login service or customers can choose to use someone registered as an Authorised Corporate Service Provider such as an accountant. To date around 900,000 people have successfully verified their identity ahead of the mandatory period which begins on 18 November.

Companies House identity verification is being introduced under the Economic Crime and Corporate Transparency Act 2023 and is not connected to the proposed new digital ID scheme. The newly announced national digital identity scheme is not yet in place and a consultation will be launched to start a national conversation on digital ID.

The purpose of our identity verification is to link verified individuals to their company roles and activity. The introduction of identity verification at Companies House will make it much harder to use the register to create anonymous corporate structures that enable fraud, corruption or other criminal activity. This is a crucial safeguard that protects everyone who uses our register, and ordinary citizens who have been at risk of having their identities stolen to facilitate fraud.

When criminals and fraudsters use fake identities to set up companies, they can quickly secure loans and commit fraud, leaving real people and real businesses to pick up the pieces.

Since March 2024 Companies House has dealt with over 100,000 reports of individuals who have been appointed as a company director or had their home address used to register a company without their consent. This can have wide reaching impacts such as damage to credit ratings, stress and distress, legal complications, administrative burdens or increased vulnerability to further fraud. Identity verification will make this much harder and will potentially stop the majority of fraudulent appointments from reaching the register.

In addition, there are business benefits to identity verification. It will play a key role in giving confidence to investors and consumers, giving greater transparency about who owns the companies the general public spend their money on. Citizens are often advised to check whether a trader is listed on Companies House and identity verification will help make sure that this listing reflects genuine and trustworthy information.

I would be grateful if you could share this clarification with your members, so they have accurate information about what Companies House identity verification is—and is not. We value constructive engagement with stakeholders, and I hope this explanation provides reassurance about our intentions.

Thank you again for your interest in our work.

Yours sincerely,

Andy King
Chief Executive Officer and Registrar of Companies for England and Wales
Companies House