Companies House consultation response: Corporate transparency and register reform

UK Finance is the collective voice for the banking and finance industry. Representing more than 250 firms, we act to enhance competitiveness, support customers and facilitate innovation.

We strongly support the proposal for fundamental reform of Companies House (CH), including verification checks of the identities of key individuals on the register, as addressing a key vulnerability in the UK regime for fighting economic crime. The private sector expends significant activity and effort into double checking CH data, detracting costs and resources from tackling high value activity to reduce economic crime. Recently the Public Private Threat Update, produced by the NECC, highlighted the abuse of companies as a significant money laundering risk. It is important that CH dedicates proper resourcing and priority to mitigating these risks in the short, medium and longer term. Government should also ensure that CH plays a full part in the wider economic crime reform agenda.

In the short term, CH should work to improve its monitoring and enforcement through the use of leading technology and by leveraging related analytical and investigatory work by civil society, anti-money laundering (AML) supervisors and public / private partnerships such as the Joint Money Laundering Intelligence Taskforce (JMLIT) and the Joint Fraud Taskforce (JFT).

In the medium term, CH reform and transformation should be aligned with related work to establish a central bank account register as required by the Fifth Money Laundering Directive (5MLD) and other information sharing and major infrastructure projects. Duplication would undermine the business case for investment and ongoing commitment of specialist resources, and in the worst case could undermine effectiveness through varying definitions and regulatory tensions.

In the longer term, the Government should prioritise improved gateways for public sector information sharing, to help CH identify material anomalies directly. Government requiring regulated firms to report to law enforcement what they, and other parts of the public sector, already know has arisen in a number of areas and results in a displacement of specialist economic crime resources away from more valuable activity.

CH reform also provides an opportunity to develop a more efficient economic crime regime, streamlining the efforts of both the public and private sectors in fighting economic crime. We also believe consideration should be given to providing access to non-public information collected by CH for regulated firms and their data providers, to facilitate compliance with their regulatory obligations

to tackle economic crime. In addition, consideration needs to be given to how the lawfulness of the data processing is addressed alongside the practical exercise of individual rights by data subjects. Consideration should also be given to allowing the regulated sector to place reliance on CH information when undertaking their own verification of customer information, once CH is itself verifying or ensuring adequate customer due diligence checks of this information.

If you have any further queries please contact nick.vanbenschoten@ukfinance.org.uk.

The case for verifying identities

Q1. Do you agree with the general premise that Companies House should have the ability to check the identity of individuals on the register? Please explain your reasons.

- Yes, we agree with this premise to encourage the reduction of key vulnerabilities. We also support the proposed scope of individuals whose identity would be subject to CH verification checks (i.e. directors, Persons with Significant Control (PSCs) and presenters). These are key roles in the establishment and operation of a company and are critical to improving CH data quality.
- We strongly support this proposal, as addressing a known vulnerability in the UK's overall framework for the domestic economy and international business. Limited CH checks of individuals' identities has proved inadequate and allowed criminals to abuse the CH register by setting up shell companies for use in a variety of economic crimes. These include use of shell companies for purchase scams and other volume fraud, and for international money laundering schemes. This vulnerability was noted in the recent Financial Action Task Force (FATF) evaluation of the UK which highlighted 'the ease with which a criminal could register inaccurate information'. The FATF recommended a list of actions to 'improve the quality of information available on the PSC register to ensure that the information is accurate and up-to-date'. Most recently, these issues were highlighted through the production of the Economic Crime Plan and Public Private threat update.
- Data quality of key CH information is critical to the overall anti-money laundering (AML) regime, as CH data on directors and PSC is a key source of customer due diligence (CDD) information for the regulated sector, both directly and indirectly via data providers. CH should apply checks both to newly presented individuals and to individuals already listed on the register, to manage both the stock and flow of data quality. We would propose that a phased approach could be taken to existing directors and PSCs, to prioritise efforts targeting higher-risk companies and other risk indicators. Verification of such CH information supports a level playing field and overall regulatory effectiveness, as verification of identity is already required

as part of CDD by company formation services by TCSPs, public notaries and other regulated sector bodies.

- CH verification of individual identities and other key information should be the default for new registration obligations, including those currently under development such as registration of overseas entities owning UK land. As stated above, such verification should also be performed for existing directors and PSCs. Our response to Q13 below considers this issue in further detail.
- CH verification of individual identities and other key information is now less costly than in the past, due to the development of innovative approaches to data analytics and AML technology solutions.

Q2. Are you aware of any other pros or cons government will need to consider in introducing identity verification?

- There are a number of pros when considering introducing identity verification:
    - Verification by CH of key information would support a more effective role for CH as part of wider integrity initiatives, including public sector data sharing and public / private partnerships. It would also support fulfilment of the Government's objectives under FATF Recommendations 24 and 25, supporting private sector efforts by facilitating access to beneficial ownership and control information.
    - Improved data quality of key CH information would support a wide range of regulatory and non-regulatory checks on companies, including consumers applying reasonable care to avoid purchase scams, commercial counter-fraud and conflict of interest procedures, public and commercial procurement controls, AML CDD, sanctions screening and anti-bribery due diligence.
    - Allows for support towards UK competitiveness via more effective business frameworks. There is a direct impact in terms of fighting fraud against individual and corporate consumers, making it harder for criminals to create sham companies and misappropriate brand names. There is also an indirect impact in terms of inward investment, contributing to greater confidence in UK corporate governance and transparency.
    - Allows for support for more innovative and secure digital sector and data services.
    - Allows for support for CH transformation programme by ensuring improved data quality for key CH information and protection of sensitive personal information. These improvements could help unlock the potential for additional CH funding streams and greater customer satisfaction through new data products and services for companies. These might include options inspired by Open Banking (e.g. enabling company

customers to allow third party provider to access non-public data via Application Processing Interfaces, for analysis and suggestion of bespoke services) and innovative approaches to financial crime risk management (e.g. a corporate KYC utility).

- The cons to consider for introducing identity verification are as follows:
    - We agree that CH verification will require additional public sector investment and ongoing running costs, to provide the necessary expertise, resourcing and system enhancements, and should be offset by an increase in fees. However, these additional costs can be managed by the use of innovative approaches to data analytics and AML technology solutions. In addition, we consider that these costs could be partly offset by additional CH funding streams developed through CH reforms and wider transformation.
    - CH funding arrangements may require additional costs to be recouped through increased fees, with a consequent impact on international competitiveness. We consider that there is significant headroom for CH fees to increase the standard fee of £12 by some multiples while remaining competitive compared to international comparators; for example, the cost of obtaining only a company seal in Ireland is €39, not counting tax registration and other fees, while the cost of registering a commercial micro-enterprise in France with the local chamber of commerce and industry is €100. The impact of fee increases on CH competitiveness could be also offset by improved protection of sensitive personal information and the development of new services and greater customer satisfaction.
    - We consider that the focus on verification of key information is important to ensure an appropriate trade-off between these pros and cons. The pursuit of data completeness and data accuracy must be treated as a means to an end, rather than an end in itself. As such, verification measures must target priority areas, such as economic crime as identified by the Public Private Threat Assessment and National Risk Assessment, and be developed in partnership with related initiatives. In the context of combatting economic crime, a risk-based approach, RBA, to verification is a critical part of the global AML regime and drives a more effective and efficient model.

Q3. Are there other options the government should consider to provide greater certainty over who is setting up, managing and controlling corporate entities?

- The Government could provide greater certainty and confidence in company set up, management and control by ensuring that CH plays a full part in the wider economic crime reform agenda. In the near term, improved CH monitoring and enforcement and future

verification could be supported, and in turn support, related analytical and investigatory work by civil society, AML supervisors and public / private partnerships such as the Joint Money Laundering Intelligence Taskforce (JMLIT) and the Joint Fraud Taskforce (JFT). In the longer term, this should include aligning CH reform and transformation with work to establish a central bank account register as required by 5MLD and other information sharing and major infrastructure projects (e.g. Suspicious Activity Reporting, SARs, reform, New Payments Architecture).

- CH should use existing economic crime typologies and information sharing initiatives to identify higher risk presenters and corporates. This would support a more intelligence-led approach to CH enforcement as well as help targeting additional CH checks and requests for additional information, in line with the RBA for AML.
- Consideration should be given to how CH could confirm, as part of a RBA, how key individuals are connected to corporate entities on the register. This could include verification of an individual's stated connections and data analysis to check for indications of unstated connections. We consider that seeking to confirm such connections would support wider CH work to identify nominee directors and nominee shareholders.
- Consideration should be given to providing access to non-public information collected by CH for regulated firms through an application and review process, as they are obliged to comply with CDD and other economic crime obligations. This could include direct access and access via Credit Reference Agencies (CRAs) and third-party providers of CDD services. Access to non-public information collected by CH could support exception-based review under a RBA, and help regulated firms identify and report material discrepancies in beneficial ownership information, reducing the volume of false positives received by CH as well as offsetting the additional costs for the regulated sector of the new identification and reporting process. However, we stress that access to additional non-public information could lead to an increase in discrepancy reporting, particularly if our feedback to Q33 and the 5MLD consultation, that the reporting obligations should not be extended beyond beneficial ownership information, is not taken into account.

- The Government should consider ways in which CH reform can provide greater transparency over the ownership and control of State-Owned Enterprises (SOEs), to support regulatory checks and risk assessment across AML, sanctions and anti-bribery requirements. This would be in line with the G20 High-Level Principles for Preventing Corruption and Ensuring Integrity in State-Owned Enterprises[1]:

[1] http://www.g20.utoronto.ca/2018/final_hlps_on_soes.pdf

- "G20 countries should design their State ownership arrangements for SOEs in a way that is supportive of high standards of integrity, including, where feasible and in accordance with domestic legal systems, *inter alia* by separating ownership from other government functions and minimising opportunities for inappropriate ad-hoc interventions and other undue influence by the State in SOEs. The ownership structure and internal transactions should, without compromising the autonomous corporate nature of SOEs, be transparent and the state should encourage professional co-operation between the relevant state authorities."

How identity verification might work in practice

Q4. Do you agree that the preferred option should be to verify identities digitally, using a leading technological solution? Please give reasons.

- Yes.
- A manual approach to verification is less efficient and would increase the time taken and administrative costs on both CH and presenters. The regulated sector uses a range of tried and tested technological solutions to meet its CDD obligations efficiently, with industry practice including widespread use of electronic documentation and reliable electronic databases. However, if CH wishes to adopt a model similar to that operating in Jersey, where the verification is outsourced to licensed formation agents which CH then monitors to ensure that appropriate standards are being met, then manual verification could be performed adequately by those agents without the same impacts on costs and delays.
- Leading technological solutions are well-suited for the type of high-volume, typically low-risk customers that currently make up the large majority of CH users. In addition to verification of the identities of key individuals, technology could help CH provide wider support such as more efficient and effective screening of these individuals for sanctions, director disqualification and wider integrity risk indicators, for example adverse media and public procurement exclusions. Leading technological solutions can also be used to identify and categorise higher risk customers requiring escalation and specialist review, including by using risk indicators developed from the AML/CTF National Risk Assessment and other threat assessments, JMLIT and financial fraud typologies and CH data analysis and information sharing with AML supervisors. Leading technological solutions could also support CH in developing a more aggressive approach to tackling economic crime. It may be useful to note that further guidance on the criteria for use of a provider of electronic verification of identity are set out in JMLSG 5.3.51.
- Consideration should be given to use of overseas third-party data providers or equivalents of CH, to ensure that chosen technological solutions can support verification of key individuals

residing overseas. This approach could be used to support checks and transparency on wider CH information (e.g. intermediate shareholding information).

- Consideration should be given to additional time and costs for verification of individuals unable to be verified by electronic identification and verification, eID&V, (e.g. under 18s, people with no credit history etc.).
- Consideration is also needed for use of E-ID solutions, both in UK and other countries.

Q5. Are there any other issues the government should take into account to ensure the verification process can be easily accessed by all potential users?

- Where users are not able to access an on-line verification process easily, use of a third-party agent seems a proportionate and tested solution.
- Consideration should be given to additional time and costs for verification of individuals unable to be verified by eID&V (e.g. under 18s, people with no credit history etc.). For example, the Post Office currently provides a document certification service to confirm that photocopied documents are a true likeness of the original. CH and professional associations can work together to help mitigate the risk of financial abuse of vulnerable users (see UK Finance Code of Practice[2] for examples of the different forms financial abuse can take.)

Q6. Do you agree that the focus should be on direct incorporations and filings if we can be confident that third party agents are undertaking customer due diligence checks? Please give reasons.

- Yes. CH should prioritise its verification efforts towards where presenters are not regulated sector bodies and where CH is not confident that regulated sector third party agents are undertaking appropriate CDD.
- We consider that, where CH is confident that third party agents are undertaking appropriate CDD, other regulated sector bodies should be able to rely on the same third-party agent checks in meeting their own CDD obligations. We also consider that this would support a more efficient economic crime regime, streamlining the efforts of both the public and private sectors by allowing resource to be allocated to more high value activity to reduce economic crime within the UK. We note that this approach would need to be underpinned by a change to Reg 28.9, to permit firms to rely on CH.
- CH should only rely on third party agents where confident in the rigour of their supervisory regime. This should include evidence of the third-party agent's regulated status with

[2] https://www.ukfinance.org.uk/financial-abuse-code-practic

additional queries and information requests made on a RBA, such as where requiring sample checks relating to thematic review findings by the third party agent's sector supervisor.

- Confidence in third party agents regulated and supervised by a non-UK AML supervisor could include an assessment of the overseas regime for equivalence and cooperation in proactive supervisory cooperation. Alternatively, CH could only rely on third party agents supervised directly by a UK AML supervisor or otherwise subject to the requirements of the 2017 MLRs (e.g. overseas branches and wholly-owned subsidiaries of regulated sector bodies in the UK).This would allow time for CH to develop a suite of questions and suitable oversight model needed to become comfortable with the agent in question. Clearly there would be a need for there to be proper oversight of company formation agents.

Q7. Do you agree that third party agents should provide evidence to Companies House that they have undertaken customer due diligence checks on individuals? Please give reasons.

- Yes.
- Consideration should be given to how CH can obtain meaningful evidence in cases where the third-party agent has completed CDD through eID&V, third party providers, CDD reliance under regulation 39 of the 2017 MLRs, etc.
- Our response to Q6 regarding third party agents regulated and supervised by a non-UK AML supervisor sets this out further.
- CH should apply a RBA to their approach, such as by targeting either their requests for evidence of CDD or their quality checking of such evidence. EBA guidance suggests criteria and examples, including sample checks in higher risk and borderline cases.
- CH should also share trend analysis and typologies with relevant AML supervisors, as part of proactive support of AML supervision for third party agents.
- In the UK, Trust and Company Service Providers (TCSPs) are regulated entities for AML and are supervised by HMRC, except where they are excluded or are supervised by another body (e.g. FCA). We consider that CH and HMRC should work closely to align their respective expectations of TCSPs and explore early opportunities for proactive joint work on monitoring and enforcement, in advance of new legislation, if needed, to enable wider public sector information sharing. Additionally, we recommend that this is linked into the upcoming threat update by the NECC on company formation.

Q8. Do you agree that more information on third party agents filing on behalf of companies should be collected? What should be collected?

- Yes.

- Examples could include whether the third-party agent has or had a role in the company, notably where they act as a nominee director or shareholder, and including where such individuals remain involved following the sale of “off the shelf” companies.
- Other examples could include the number of companies that a third-party agent has established (excluding off-the-shelf) and details of the jurisdictions in which their PSC resides (focusing on higher risk locations). Further information could be requested on a RBA, such as details of the third party agent’s systems and controls to manage economic crime risks.

Q9. What information about third party agents should be available on the register?

- The register should make available information on:
    - Whether the company was presented by a third-party agent;
    - Whether CH relied on the CDD of a third-party agent;
    - Whether a third-party agent regulated and supervised overseas was used, and, if so, their regulatory authority and registration number; and
    - Other companies within the register that the third party is associated with. This would help regulated entities take steps to respond to indications that a third party agent is abusing the register or has otherwise raised suspicions.

Who identity verification would apply to and when

Q10. Do you agree that government should (i) mandate ID verification for directors and (ii) require that verification takes place before a person can validly be appointed as a director? Please set out your reasons

- Yes.
- Rights and responsibilities as a publicly listed director create economic crime risks that should be managed effectively. In addition to ID verification, CH should apply leading technology to screen directors for sanctions, director disqualification and wider integrity risk indicators, such as adverse media and public procurement exclusions.
- Consideration should be given to which aspects of identity are to be verified (e.g. name, address, date of birth, etc.). CH should then apply a RBA to the verification of these aspects of identity and other relevant checks, before a person can be appointed as a director.
- Consideration should be given to what would be the process where one/some proposed director(s) fails verification but others pass (i.e. should that Company be incorporated).CH verification of individual identities and other key information should be the default for new registration obligations, including those currently under development, such as registration of overseas entities owning UK land.

- Regulated sector bodies are required, as part of their CDD obligations for corporate customers, to take reasonable measures to determine and verify the full names of the board of directors. If CH verifies the identity of directors in line with regulatory expectations, we consider that regulated sector bodies should be able to rely on these checks as they work to comply with their CDD obligations. We also consider that this would support a more efficient economic crime regime, streamlining the efforts of both the public and private sectors in fighting economic crime. This would, once again, need to be underpinned by a change to Reg 28.9.

Q11.How can verification of People with Significant Control be best achieved, and what would be the appropriate sanction for non-compliance?

- The technological solutions outlined in response to Q4 above should similarly be applied to the verification of PSCs.
- In order to focus resource on higher risk priorities and to support wider economic crime initiatives, Government could supplement CH verification with support from AML supervisors and from public / private partnerships such as JMLIT and JFT. This would allow the use of economic crime typologies and information sharing to identify higher risk presenters and corporates and target additional checks, in line with the RBA for AML.
- Risk-based proactive monitoring and enforcement are at least as important as the level of sanction. Greater publicity of CH enforcement could also encourage compliance. From members experience of routine CDD review, corporate customers frequently delay updating their CH filings until requested to do so by regulated service providers.
- CH business planning should provide for a robust and flexible enforcement toolkit, in line with the recommendations of the Macrory Review. Consideration should also be given to ring-fenced resourcing of multi-agency partnerships and sustained targeting of more frequent repeated and egregious non-compliance.
- Given the range of economic advantages provided by CH registration, compliance could be accelerated progression through a spectrum of adverse consequences including adverse publicity and referrals to other agencies. These might include flagging on the register where there were unanswered queries about PSC information, administrative penalties for delayed answers and late updates, targeted use of enforcement undertakings for unintentional but negligent non-compliance, civil sanctioning powers for repeated or reckless non-compliance, and close cooperation with LEAs and AML supervisors for suspicious non-compliance.

Q12. Do you agree that government should require presenters to undergo identity verification and not accept proposed incorporations or filing updates from non-verified persons? Please explain your reasons.

- Yes.
- Identification and verification of non-regulated presenters will support wider counter-fraud controls and procedures against company hijacking, identity theft and impersonation fraud, including consultation proposals to check that presenters are authorised to act on behalf of the company and to use the company name.
- Identification and verification of regulated third party agents will support proactive CH support for AML supervision of these sectors, as well as supporting counter-fraud controls.

Q13. Do you agree with the principle that identity checks should be extended to existing directors and People with Significant Control? Please give reasons.

- Yes. CH should apply checks both to newly registered individuals and to existing individuals, to manage both the stock and flow of data quality.
- However, a phased and RBA, in line with existing reporting obligations, should be taken to existing directors and PSCs, to prioritise efforts targeting higher-risk companies and other risk indicators. The private sector has extensive experience in undertaking large-scale remediation projects, including the use of leading technology. We consider that many of the lessons learned will be transferrable to CH planning and scoping of their own remediation work.
- A RBA could include an exception-based approach to dormant and dissolved companies, initially only prioritising verification for directors and PSCs of dormant and dissolved companies where associated with multiple high-risk indicators and specific typologies. Where an existing corporate entity seeks to amend or update their registry information this could be an opportunity for CH to require verification of the identity of key individuals.
- CH verification of individual identities and other key information should be the default for new registration obligations, including those currently under development such as registration of overseas entities owning UK land.

Requiring better information about shareholders

Q14. Should companies be required to collect and file more detailed information about shareholders?

- Yes.

- Sufficient information should be collected to enable CH to identify the shareholder as an individual and link their exposure across other companies already registered on CH.
- Consideration should be given to how additional information requirements about shareholders will affect time-sensitive customers, such as in relation to mergers and acquisitions.
- Consideration should be given to how CH will encourage compliance with existing and new filing requirements. From members experience of routine CDD review, corporate customers frequently delay updating their CH filings until requested to do so by regulated service providers.

Q15. Do you agree with the proposed information requirements and what, if any, of this information should appear on the register?

- Yes.
- Name, date of birth and residential address information are a useful data set for economic crime screening, including financial sanctions screening. For companies and other legal entities, useful information would include registered name, registration number, registered address and, if different, its principal place of business. Where available, Legal Entity Identifier (LEI) codes would also be useful.
- If some of this personal information was protected from public disclosure on the register, then consideration should be given to disclosing the protected information to regulated firms and others obliged to comply with CDD and economic crime screening. We note that it is crucial to consider the balance between personal data privacy and the public interest in economic crime here.
- Access to non-public information collected by CH could support exception-based review under a RBA and help regulated firms identify and report material discrepancies in beneficial ownership information, reducing the volume of false positives received by CH as well as offsetting the additional costs for the regulated sector of the new identification and reporting process.

Q16. Do you agree that identity checks should be optional for shareholders, but that the register makes clear whether they have or have not verified their identity? Please give reasons.

- Identify checks should be optional for shareholders under a defined threshold. For example, a 5% threshold would align with the disclosure threshold for traded shares. However, industry practice varies between 10 – 25% dependent on the risk of the customer. A 25% threshold could therefore be more closely aligned with industry practice for financial and banking sector CDD checks on beneficial ownership, as well as GDPR.

- Where shareholders under the threshold are not subject to identity checks, this should be flagged on the register.
- Consideration should be given to how additional information requirements about shareholders will affect time-sensitive customers, such as in relation to mergers and acquisitions.

Linking identities on the register

Q17. Do you agree that verification of a person's identity is a better way to link appointments than unique identifiers?

- Yes. There are a number of challenges to linking identities, as noted below, but we consider that verification of identity is preferable to unique identifiers.
- Linking appointments via verification of a person's identity will require a consistent approach from CH on how to address variations in a persons' name between different sources of ID/AV documentation (e.g. minor spelling variations, hyphens and spaces in double barrelled names, truncated names, joint bank accounts, etc). The same issue arises in the 5MLD requirement for regulated firms to notify CH of discrepancies between CH beneficial ownership information and the firms' CDD information, and in the roll-out of the Confirmation of Payee service.
- Directors and PSCs may provide different verification sources and thus it may not be straight-forward to connect the same identity from verification sources alone.
- Similar challenges are likely to arise for linking identities under the 5MLD requirement to establish a central bank account register. However, there are also opportunities for this 5MLD project to support CH reform through streamlined data feeds and cross-checking. We strongly encourage CH to play a full part in the wider economic crime reform agenda and align with the central bank account register and other information sharing and major infrastructure projects (e.g. SARs reform, New Payments Architecture).

Q18. Do you agree that government should extend Companies House's ability to disclose residential address information to outside partners to support core services?

- Yes.
- Disclosure to outside partners should include economic crime public / private partnerships such as JMLIT and JFT.
- Consideration should be given to disclosing residential address information to regulated firms and others obliged to comply CDD and wider economic crime requirements (e.g. screening for financial sanctions compliance).

Reform of the powers over information filed on the register

Q19. Do you agree that Companies House should have more discretion to query information before it is placed on the register, and to ask for evidence where appropriate?

- Yes.
- CH could target its queries and requests for evidence with support from AML supervisors and from public / private partnerships such as JMLIT and JFT. Use of economic crime typologies and information sharing to identify higher risk presenters and corporates and target additional checks, in line with the RBA for AML.
- Consideration should be given to how these queries are presented on the public register. For example, if accounts are submitted and a query raised, will these then appear as overdue on the public register or will then be flagged as under review? There should also be some timeframes in place around the raising of a query / request for evidence by CH and the response being provided by the company. Where this is not met then this would need to be viewable on the public register and also consideration given to sanctions for the company.
- It would be helpful to have a list of companies that CH have requested more information from in one place.
- There needs to be an agreed approach towards companies that appear flagged on CH. If there are flags against companies for non-compliance, where for example the above scenarios are not met, should those flags be considered an “adverse media” hit for obliged entities? There needs to be a clear distinction between flags for pending queries and flags for non-compliance to ensure that these are clearly actionable for obliged entities.

Q20. Do you agree that companies must evidence any objection to an application from a third party to remove information from its filings?

- Yes.
- Threshold for credible, factual evidence should be designed with input from the Joint Fraud Taskforce, to support efficient and effective action against high-volume fraud. We note banks experience of collaboration with telecoms and internet service providers addressing system vulnerabilities in other sectors, such as spoofing text messages and fraudulent internet domains.

Reform of company accounts

Q21. Do you agree that Companies House should explore the introduction of minimum tagging standards?

- Yes.

Q22. Do you agree that there should be a limit to the number of times a company can shorten its accounting reference period? If so, what should the limit be?

- Yes.
- Members agree that repeated use of this provision is an indication that a company is experiencing financial difficulties or has some other reason to conceal the extent of their assets and liabilities.
- We recommend prohibition on repeated shortening within a set period, to ensure appropriate accounting transparency (e.g. only allowing shortening once every three years). Limited exceptions could be envisaged if supported by an application and CH review process.

Q23. How can the financial information available on the register be improved? What would be the benefit?

- More active CH monitoring and enforcement could encourage compliance with financial information filing requirements. From members experience of routine CDD review, corporate customers frequently delay updating their CH filings until requested to do so by regulated service providers.
- Consideration should be given as to how the UK Single Electronic Format can be leveraged across other Government departments – such as HMRC. This could help reduce the friction for the users, and also reduce the risk of misleading appearance of liquidity or tax avoidance (e.g. through use of bespoke accounts prepared for each department).

Clarifying People with Significant Control exemptions

Q24. Should some additional basic information be required about companies that are exempt from People with Significant Control requirements, and companies owned and controlled by a relevant legal entity that is exempt?

- Yes.
- Reliable basic information is already publicly available about Relevant Legal Entities listed on an equivalent regulated market, due to these entities being subject to reliable disclosure regimes (i.e. equivalent to the Markets in Financial Services Directive / MFID). However, Relevant Legal Entities listed in non-equivalent regulated markets will not be subject to these reliable disclosure regimes so it would be valuable for the register to require additional basic information. Through public sector information sharing and peer learning, CH is well placed to design and check additional information relating to regulated markets. Consideration

should be given to CH making its assessment of what constitutes a 'regulated market' available to regulated sector bodies.

Dissolved company records

Q25. Do you agree that company records should be kept on the register for 20 years from the company's dissolution? If not, what period would be appropriate and why?

- Yes.
- We would question whether there is a GDPR retention element for CH to consider here.
- In aligning with the 5MLD requirement that PSC information should only be retained for a maximum of 10 years after dissolution, consideration could be given to mixed approaches. For example, retaining PSC information longer than 10 years if related to regulatory enforcement or specific higher-risk indicators, and/ or restricting access to PSC information more than 10 years after dissolution for regulated firms only.
- Additionally, we flag the case of phoenix companies, where directors liquidate companies and then re-form new ones. If CH were able to monitor this through dissolved or insolvent companies records, it would have a positive impact on economic crime prevention.

Public and non-public information

Q26. Are the controls on access to further information collected by Companies House under these proposals appropriate? If not, please give reasons and suggest alternative controls?

- No.
- CH should ensure that law enforcement and AML supervisors have the necessary information sharing gateways to access all information collected by CH. These gateways should be supported by data held in a searchable format.
- Consideration should be given to providing access to non-public information for regulated firms, as obliged to comply with CDD and other economic crime obligations. Access to non-public information collected by CH could support exception-based review under a RBA and help regulated firms identify and report material discrepancies in beneficial ownership information, reducing the volume of false positives received by CH as well as offsetting the additional costs for the regulated sector of the new identification and reporting process.
- We note that UK law enforcement will have timely access to UK bank accounts through the 5MLD requirement to establish a central bank account register, which could help populate and check further information collected by CH. This could reduce unnecessary duplication and help streamline efforts of both public and private sectors in fighting economic crime. CH should play a full part in the wider economic crime reform agenda, and align with this 5MLD

project and other information sharing and major infrastructure projects (e.g. SARs reform, New Payments Architecture).

- We agree that information about a company's bank account(s) is liable to be abused to enable fraud and wider crime and should be restricted through an application and CH review process.
- We note that there is a wider point around general data privacy here. Considering the register could include personal information, which could aid the perpetuation of fraud, we stress that adequate thought be given to how data would be protected and restriction criteria applied.

Information on directors

Q27. Is there a value in having information on the register about a director's occupation? If so, what is this information used for?

- There are mixed views from members here. Some members consider that, depending on data quality, regulated sector bodies may utilise this information to corroborate source of wealth information provided by an individual customer or by persons behind corporate customers.
- Other members view this information as of limited use for risk assessment, CDD and identification and determination of criminal networks.

Q28. Should directors be able to apply to Companies House to have the "day" element of their date of birth suppressed on the register where this information was filed before October 2015?

- Yes, but consideration should be given to disclosing this protected information to regulated firms and others obliged to comply with CDD and wider economic crime requirements.
- Access to non-public information collected by CH could support exception-based review under a RBA and help regulated firms identify and report material discrepancies in beneficial ownership information, reducing the volume of false positives received by CH, as well as offsetting the additional costs for the regulated sector of the new identification and reporting process.

Q29. Should a person who has changed their name following a change in gender be able to apply to have their previous name hidden on the public register and replaced with their new name?

- Yes, but consideration should be given to disclosing this protected information to regulated firms and others obliged to comply with CDD and wider economic crime requirements.
- The principles of the Gender Recognition Act 2004 should be applied.

- We consider that access to such protected information in order comply with economic crime requirements would support regulatory and public policy objectives for financial inclusion and treating customers fairly. Some individuals will have changed their name without use of formal legal documentation, such as deed poll, and access to such protected information would help regulated banking and financial firms minimise delays and intrusive requests for additional information and documentation.

Q30. Should people be able to apply to have information about a historic registered office address suppressed where this is their residential address? If not, what use is this information to third parties?

- Yes, but consideration should be given to disclosing this protected information to regulated firms and others obliged to comply with CDD, identify sham companies used to facilitate purchase scams and other volume frauds, and for wider economic crime requirements.

Q31. Should people be able to apply to have their signatures suppressed on the register? If not, what use is this information to third parties?

- Yes, but consideration should be given to disclosing this protected information to regulated firms and others obliged to establish controls to counter the risk of their firm being used to further fraud and identity theft, and wider economic crime requirements.

Compliance, intelligence and data sharing

Q32. Do you agree that there is value in Companies House comparing its data against other data sets held by public and private sector bodies? If so, which data sets are appropriate?

- Yes.
- CH should ensure that law enforcement and AML supervisors have the necessary information sharing gateways to access all information collected by CH. For example, if the FCA or HMRC is taking enforcement action against a company that also provides company registration services this may be relevant to the sampling and oversight approach CH may seek to take to their registrations. Existing economic crime typologies can help prioritise data sets for use with public / private partnerships such as JMLIT, DCPCU and JFT.

Q33. Do you agree that AML regulated entities should be required to report anomalies to Companies House? How should this work and what information should it cover?

- Yes, only in relation to material discrepancies identified through existing CDD processes in line with the explicit requirements laid out in the 5MLD (please see at Annex an excerpt of

our response to this aspect of HM Treasury's consultation on the approach to 5MLD transposition). We do not support the gold-plating of these requirements beyond beneficial ownership information, and do not consider that the additional CH reporting requirement should be pursued.

- Firstly, we consider that this CH reporting requirement would exacerbate risks of unintended consequences for companies, regulated firms and the wider fight against economic crime. As noted in our response to the HM Treasury consultation on the approach to implementing related requirements under the 5th Money Laundering Directive (5MLD), it is important that Government takes a holistic and proportionate approach to the introduction of new reporting obligations on AML regulated entities to manage risks of unintended consequences. For example, the risk of overbroad definitions of 'discrepancy' resulting in disproportionate burdens and delays on standard onboarding and monitoring procedures, including simplified due diligence in low-risk business relationships, and the risk of imposing duplicative efforts across the market would disrupt standard CDD practice such as use of third-party providers and reliance on CDD information provided by another regulated firm. These disproportionate burdens and delays would also impact on CH through a higher volume of reported discrepancies that had little or no material relevance to potential fraud or other criminal abuse of the register, and potentially distract CH resources from the scrutiny of more significant data quality issues. We consider that these risks would be significantly more complex to manage if the 5MLD reporting requirement were extended to all company registration information held on the CH register, as per the proposed CH reporting requirement.
- Secondly, we consider that this CH reporting requirement stands in need of specific justification. The related 5MLD requirement is limited to requiring regulated firms to report discrepancies between PSC information in the register and the CDD information available to regulated firm. The CH consultation proposals go beyond 5MLD requirements and are therefore gold plating. The CH proposal should therefore be justified in terms of being required to mitigate a material ML/TF risk, as well as a clear cost / benefit analysis.
- Thirdly, we consider that the proposed reporting requirement will be ineffective as based on misunderstandings about current market practice in meeting CDD requirements. For example the 2017 MLRs prohibit sole reliance on PSC information in the register for CDD purposes. As a result, some regulated firms will not be using CH data, and this may be suppressing current reporting of discrepancies. This prohibition should be revisited in future, in light of public sector verification and data quality sampling.
- We also note that CDD does not require verification of all areas of the register, limiting the value of a mandatory feedback loop. Imposing an additional mandatory requirement to obtain and check all areas of the register would impose disproportionate costs, including diversion

of specialist AML expertise away from higher value activity and increased delays to legitimate corporate customers.

- If CH has identified material risks arising from anomalies from areas of the register not verified as part of the CDD process, then we would strongly urge a more targeted and proportionate approach to defining and addressing these risks. This is particularly important given the number of major infrastructure projects currently under development relevant to economic crime that could support a more efficient and effective approach, such as the 5MLD requirement to establish a central bank account register.
- For example, more active CH monitoring and enforcement could encourage compliance with financial information filing requirements. From members experience of routine CDD review, corporate customers frequently delay updating their CH filings until requested to do so by regulated service providers.
- Public-private partnership work with professional associations for accountants and auditors could also help CH address any material risks of anomalies in the wider register. For example, CH might develop its approach to verification and monitoring through use of accountancy sector risk typologies and information sharing (e.g. through a new JMLIT group for the regulated accountancy sector).
- Finally, the Government should prioritise improved gateways for public sector information sharing to help CH identify material anomalies (e.g. between accounts registered with CH, HMRC, etc). The problem of requiring regulated firms to report to law enforcement what law enforcement already know has arisen in a number of areas and is starting to be addressed through reform of the Suspicious Activity Reporting regime. We strongly urge the Government to apply lessons learned and avoid unnecessarily and costly over-reporting.

Q34 Do you agree that information collected by Companies House should be proactively made available to law enforcement agencies, when certain conditions are met?

- Yes.
- Information should also be proactively made available to JMLIT, DCPCU, JFT and other public / private partnerships. Likewise, CH should leverage existing intelligence sharing (such as JMLIT) to provide an insight into how companies are being abused to better enable a RBA to how the data held by CH is viewed and monitored. Consideration should be given to providing access for regulated firms, as obliged to comply with CDD and other economic crime obligations. Existing economic crime typologies can help prioritise types of information.
- Consideration should be given to how a consistently proactive approach will be overseen and incentivised. Although CH analyse data on the request of law enforcement agencies, there are examples where a more proactive data analysis regime would act as a tool for detection

and deterrence, for example, analysing high velocity and high-volume submitters and directors (such as Barbara Kahan) and the IP address of submitters. Options could include NECC powers of direction, next steps for the Law Commission review of the Proceeds of Crime Act (POCA) and review of the 2017 MLRs.

Q35. Should companies be required to file details of their bank account(s) with Companies House? If so, is there any information about the account which should be publicly available?

- We agree that information about a company's bank account(s) is liable to be abused to enable fraud and wider crime. Access should be restricted to public agencies, with access for CRAs and regulated firms through an application and CH review process.
- As noted in our response to Question 33 above, we do not consider that the additional CH reporting requirement should be pursued. This includes the suggestion at paragraph 222 of the CH consultation that banks and other regulated sector bodies should be obliged to check and report discrepancies in companies' reported bank accounts.
- We consider that public sector data sharing and cross-checking would provide a more effective approach, such as through CH reform aligning with the 5MLD requirement to establish a central bank account register. We note that the high turnover of bank accounts in the SME sector usually reflects the customer seeking to benefit from special offers made available to new customers, rather than any financial crime efforts.
- We note that the body corporate will usually apply for a bank account only after the body corporate has been incorporated. In these instances, body corporates should provide CH with relevant details once approved by the respective bank.
- The register should flag where a company only has an overseas bank account.

Other measures to deter abuse of corporate entities

Q36. Are there examples which may be evidence of suspicious or fraudulent activity, not set out in this consultation, and where action is warranted?

- More detailed consideration needs to be given around limiting numbers of companies at a single address, given there are TCSPs which operate from 'service address' locations, who in turn then offer postal services to a large number of companies. This is opaque, but not necessarily an indicator of crime. One option would be for CH to determine a threshold for numbers of companies at a single address, to trigger additional review &/or requests for information. However, we would stress the importance of ensuring that this did not disproportionately impact small businesses. Additionally, CH could consider "blacklisting" certain addresses.

- The proposed changes are focused on managing risk where there are individuals behind a company, but the risks around a company being a director or PSC remain in place and the consultation does not address this issue. The risk is especially high where the company is registered in less transparent jurisdictions.
- Consideration should be given to how financial crime typologies will evolve in light of the proposed changes. This will require a view on how CH uses its data to monitor changes in behaviour and understand the risks associated with those changes – which may also be supported by participating in intelligence sharing fora to gain insights across the public and private sector.

Q37. Do you agree that the courts should be able to order a limited partnership to no longer carry on its business activities if it is in the public interest to do so?

- Yes.

Q38. If so, what should be the grounds for an application to the court and who should be able to apply to court?

- Grounds for an application should be designed with input from JMLIT, DCPCU and JFT, to support efficient and effective action against the criminal misuse of limited partnerships.
- The application should be accessible to all, but the level of proof cannot align to a criminal conviction because this will not address the overseas challenge raised in the CH consultation at paragraph 224. A balance of evidence comparable to a civil case may therefore be more proportionate.
- Consideration should also be given as to whether an individual should carry the burden of proof solely or whether they can make an application to CH to develop a case on their behalf. Where the process is too burdensome or expensive for individuals then it won't be used and thus the system will remain open to companies remaining active where it is not in the public interest.

Q39. Do you agree that companies should provide evidence that they are entitled to use an address as their registered office?

- Yes.
- Challenges may be raised for companies that are forming and are yet to have proof of their address, which in turn may lead to more use of serviced addresses and use of TCSP addresses – which then feeds into the issued flagged through Q36.

- However, there are established routes for ‘anti impersonation’ checks to be completed which the regulated sector already follows. CH could consider replicating these as a method of detecting misuse at an early stage in the company lifecycle.

Q40. Is it sufficient to identify and report the number of directorships held by an individual, or should a cap be introduced? If you support the introduction of a cap, what should the maximum be?

- High volume directorships are a risk indicator for economic crime, as well as for inadequate corporate governance.
- There are sometimes valid reasons for multiple dictatorships, such as liquidation, which may not be addressed through a cap. Therefore, we recommend CH should set a threshold to trigger further review and/or information requests.
- International benchmarking would support a workable cap or threshold, and international consistency would help simplify cross-border compliance. Some other financial centres have set a cap of 5 directorships (e.g. Singapore).
- Consideration should be given to the potential for unintended consequences from setting a defined limit or further review based on the number of directorships that can be held by an individual. Where a criminal group can no longer use a single director many times then they will seek to use ‘mule’ directors. A single director with a high number of companies is easy to identify in the data set and review and determine whether suspicion can be formed. Once this is fragmented into many unrelated directors, the ability to identify the suspicion or the network may be lost.
- To mitigate these risks, the use of limits or thresholds could be supported by other analytics to identify unusual / suspicious activity such as IP address tracking.

Q41. Should exemptions be available, based on company activity or other criteria?

- Yes, subject to application and CH review.
- Third party agents producing ‘off-the-shelf’ companies for future sale should be required to apply for an exemption. Consideration should be given to whether such agents producing ‘off-the-shelf’ companies should be required to provide additional compliance reports to both CH and their AML supervisor.

Q42. Should Companies House have more discretion to query and possibly reject applications to use a company name, rather than relying on its post-registration powers?

- Yes.

- Concerns regarding misuse of a company name should be resolved prior to registration to reduce the risk that the genuine company (or its customers) are defrauded in the interim. CH discretion should include the identification and challenge of similar-sounding company names, as these can enable volume fraud. Purchase scams are a high-volume and increasing fraud type, often enabled by websites and bank accounts set up to resemble well-known and trusted merchants through the use of similar-sounding company names.

Q43. What would be the impact if Companies House changed the way it certifies information available on the register?

- The register should support confidence in company information by flagging where a company is undergoing enforcement or has had a material discrepancy reported against it.
- The Register should also flag specific risk indicators, such as where a company has been established by a third-party agent not supervised in the UK & where a company only has an overseas bank account.

Q44. Do you have any evidence of inappropriate use of Good Standing statements?

No comment.

AOB

- We recognise the requirement for primary legislation in some areas. However, CH should take urgent action in priority areas as far as possible within existing powers (e.g. through appropriate use of existing information sharing gateways, public / private partnerships, etc).
- The banking and financial sector stand ready to support proofs-of-concept to help CH develop new typologies for economic crime risk, provide proactive support to AML supervisors and address misuse of well-known company names.
- We stress once again that CH should also play a full part in the wider economic crime reform agenda, and align with other information sharing and major infrastructure projects (e.g. 5MLD bank account register, SARs reform, New Payments Architecture).

ANNEX – excerpt from UK Finance response to Chapter 8 of the HM Treasury consultation on the approach to transposition of the 5th Money Laundering Directive

*This excerpt relates to the requirements of the 5MLD, which looks at the reporting of discrepancies in beneficial ownership information **only.** The consultation asks the following questions:*

> *61 Do you have any views on the proposal to require obliged entities to directly inform Companies House of any discrepancies between the beneficial ownership information they hold, and information held on the public register at Companies House?*
>
> *62 Do you have any views on the proposal to require competent authorities to directly inform Companies House of any discrepancies between the beneficial ownership information they hold, and information held on the public register at Companies House?*
>
> *63 How should discrepancies in beneficial ownership information be handled and resolved, and would a public warning on the register be appropriate? Could this create tipping off issues?*

- It is important to note that financial institutions do currently provide feedback, although we understand that this is on the basis of saliency on a risk-based approach, with complications as below. The proposals in this chapter do not reflect a practical understanding of the current industry approach to sourcing beneficial ownership information. Common practice involves the use of third- party providers for CDD information. However, these providers themselves tend to source information from registers such as Companies House. Therefore, the likelihood of additional information being held within the private sector is not as high as suggested within the consultation. Further, where discrepancies are noted between information held on the client and that provided by the third-party data provider, contact will often be made by the third-party provider to confirm this information with Companies House, rather than by the financial institution. There is a concern that these requirements may mandate duplicative efforts across involved parties. We urge that the regulations need to acknowledge industry practice and technological options here and ensure that innovation is not stifled; particularly across third party providers delivering this service to the regulated sector.
- It is important that the new reporting requirement does not undermine the risk-based approach and impose disproportionate burdens on standard onboarding and monitoring procedures, including simplified due diligence in low-risk business relationships, use of third-party providers and reliance on CDD information provided by another regulated firm.
- Whilst the proposal for the reporting mechanism to involve entities informing Companies House of discrepancies is generally supported, we stress that it is essential this is clearly defined to ensure that this exercise is not used as an excuse for private sector entities to hold responsibility for fixing data quality issues within Companies House itself. We note that there is already

legislation in place which obliges companies and trusts to ensure information is recorded accurately at Companies House and updated in a timely fashion where changes arise, and we consider that Companies House could do more to incentivise compliance directly with companies and trusts. It is therefore important that the reporting mechanism is implemented to support Companies House reform and is not treated as extending the gatekeeping obligation to regulated firms, which would ultimately become de facto agents of Companies House. Our members also have some reservations as to the capacity of Companies House to effectively manage the potential influx of discrepancy reporting.

- Not least, criminals only need to be consistent in false information provided to obliged entities and Companies House to avoid detection, so there remains a question on how effective this mechanism is from a financial crime perspective.
- Crucial to this will be defining the scope of "discrepancy" We propose that discrepancies are looked at across three categories:
    - Minor discrepancies; e.g. typos, missing hyphens;
    - Discrepancies requiring further investigation, when it is unclear whether the discrepancy is material; e.g. time lags following applications to update information on the register, and other low risk anomalies;
    - Material discrepancies; e.g. evidence of red flags, evidence of previously unidentified individuals.
- We propose that discrepancies are categorised across the above on a case by case basis, in line with a risk- based approach. This is crucial to ensure proportionality in reporting, to ensure avoidance of reporting discrepancies on the vast majority of companies that pose no ML/TF risk. We understand that some other Member States are taking a similarly proportionate approach to transposition of the new reporting requirement, including defining reportable discrepancies in terms of where the firm has "reasonable doubt" in the accuracy or absence of beneficial owner information on their register.
- Once categorised, all major discrepancies should be reported to Companies House within a short but practicable time frame after being categorised. The discrepancies falling into the further investigation category must also be reported within a reasonable timeframe unless discounted as typos. We note that the consultation is silent on the timeframe and process for the reporting and we consider that any new reporting requirement should support proportionate and workable approaches, such as periodic bulk reporting in the majority of cases.
- We stress that it should not be mandated that obliged entities must report the discrepancy immediately. Clarification needs to be provided regarding how quickly discrepancies are required to be reported (e.g. do they need to be reported immediately, can they be sent in bulk on a batch

basis, can the approach vary by risk or some other criterion, etc.). We consider that it should not be mandated that obliged entities must report the discrepancy immediately in all instances; e.g.:

  - When the obliged entity is already aware that the customer's beneficial owners are about to change/have just changed and the customer is in the process of updating this information (e.g. management buy-out);
  - When the customer has already reported the discrepancy to Companies House but it has not yet been updated on the register.

- We believe in these scenarios, given the existing obligations for customers themselves to update Companies House, it is more appropriate for regulated firms to report discrepancies only if and when the customer does not update the register and the regulated firm considers such behaviour material (e.g. missing beneficial owners) and/or suspicious.
- We note the need to manage the potential commercial and customer impacts of this proposal, whereby delays by Companies House in verifying the data in question would require disproportionate manual review and cause delay in bank onboarding processes with the customer, or indeed any other part of the customer journey. We strongly urge that discrepancies should not have any impact on onboarding once an obliged entity is satisfied they have completed the necessary due diligence; e.g. firms identifying discrepancies in low-risk customers with no impact on their risk assessment of the business relationship should be able to apply simplified due diligence. If an obliged entity is comfortable that it has identified and taken reasonable steps to verify the identity of the beneficial owner(s) (e.g. through obtaining the share register) then it has met its regulatory obligations and can proceed with onboarding, even if the register is discrepant. Commonly, the obliged entity would discuss the discrepancy with the customer and subsequently check that they have updated it. We also propose that firms placing reliance on another firms' onboarding CDD or making use of a third-party provider should not be required to duplicate the process for identifying and reporting discrepancies.
- Further, the Government should take into account duplicative reporting by multiple obliged entities (and the additional, non-productive, work that will be the result for Companies House). If a 'non-compliant' flag is added to the Companies House entry, it would make sense that obliged entities need not report discrepancies until that flag is removed.
- It is essential for proportionality and workability that the requirement to report discrepant information does not introduce a new obligation to check all information on the register. We consider that such a wider obligation is gold plating of the 5MLD and that it is not justified in terms of being required to mitigate a material ML/TF risk. It must be clear that the obligation is to report a discrepancy when it is identified through the obligated entity's due diligence processes.
- Clarification is required on whether the requirement to report discrepancies is restricted to reporting the obliged entity's customer when conducting due diligence, or whether it extends to

other circumstances (e.g. to the customer's parent company, or when discrepancies are identified through intelligence-based investigations such as JMLIT or court orders). In such other cases, law enforcement may already be aware of the discrepancy and may not want it to be reported to Companies House. There is also a question of efficiency. The problem of requiring regulated firms to report to law enforcement what law enforcement already know has arisen in a number of areas and is being addressed through SARs reform. We strongly urge the Government to apply lessons learned and avoid unnecessarily and costly over-reporting.

- We also note the need to manage the potential market impacts of this proposal, whereby a lack of regulatory clarity over definitions and requirements would drive inconsistent market practice.
- More clarity required on how long it would take CH to resolve discrepancies considering, dependent on how this is defined, the number could be numerous; what Companies House will do with the information provided by an obliged entity; how Companies House intend to validate this information with companies, and whether Companies House would advise obliged entities when Companies House is updated.
- We recommend that HMT, Companies House and BEIS reflect on the commonalities between reporting discrepancies to Companies House and the known issues of the suspicious activity reporting regime as highlighted by the Law Commission's review of POCA (e.g. duplicative reporting, reporting what Companies House already knows, or over reporting in the absence of clear guidance).
- In terms of resolving discrepancies, it would also be crucial for there to be some sort of feedback loop back from Companies House to the reporting entity, to confirm whether the discrepancy information was valid or not. We trust that the public sector commitment ensures there is resource within the reformed Companies House structure to do this.
- Obliged entities will need to understand the service level agreements (SLA) that Companies House has to investigate and resolve a reported discrepancy. We suggest that the 'non-complaint' flag should be an indication to the reporting obliged entity that their reported discrepancy is still under investigation. Should the flag be removed without the data attributes being corrected by Companies House, it is likely that the obliged entity will have an obligation to report the discrepancy for a second time.
- We consider that the new reporting requirement should not apply where firms have reported suspicions of money laundering and noted discrepancies in Companies House beneficial ownership information. In such cases there should be information sharing arrangements between the UK Financial Intelligence Unit and Companies House to allow information on the suspicious discrepancies to be shared, in support of Companies House compliance and enforcement activity.