1 Angel Court,
London, EC2R 7HJ
ukfinance.org.uk

Darren Jones MP
Chair, Business, Energy and Industrial Strategy Committee
House of Commons
Westminster
SW1A 0AA

By Email: FOXK@parliament.uk

21 December 2022

Dear Darren,

Thank you for the opportunity for UK Finance to give oral evidence to the BEIS Select Committee's non-inquiry session of 8th November on fraudulent company registrations and the Economic Crime and Corporate Transparency Bill.

UK Finance welcomes the Select Committee's scrutiny of the Economic Crime and Corporate Transparency Bill's provisions for Companies House reform and information sharing on economic crime within the regulated sector. This type of reform would help make the UK a safer and more transparent place to do business.

I offered to provide further written evidence on the tools and procedures used by the banking sector to prevent and detect financial fraud. As noted in our oral evidence, fraudulent business accounts constitute a relatively small part of the financial fraud threat we see in comparison to millions of cases annually of unauthorised and authorised payment fraud, but we recognise the devastating impact fraud has on victims. Monies stolen through fraud also fund serious organised crime and impact the wider economy.

Banks take their customer due diligence responsibilities very seriously, investing billions of pounds each year in preventative and monitoring systems, working with law enforcement to share intelligence and responding collectively to emerging trends in fraudulent activity.

Before opening business accounts, banks undertake customer due diligence on the business entity and its key account parties in accordance with the requirements of the UK Money Laundering Regulations[1] and the supporting guidance of the Joint Money Laundering Steering Group (JMLSG)[2].

This includes verification of the identity of the business entity and its key account parties on the basis of documents or information obtained from a reliable source, which is independent of the customer.

---

[1] https://www.legislation.gov.uk/uksi/2017/692/contents

[2] https://www.jmlsg.org.uk/guidance/current-guidance/

In many situations firms need to be prepared to accept a range of documents but will apply procedures to check for counterfeit documents and to establish whether any suspicious documents have been reported as lost or stolen.

Evidence can include identity documents issued by government departments and agencies, such as passports and photograph driving licenses, but documentation from other sources can also be used. There is a broad hierarchy of documents:

- certain documents issued by government departments and agencies, or by a court; then
- certain documents issued by other public sector bodies or local authorities; then
- certain documents issued by regulated firms in the financial services sector; then
- those issued by other firms subject to the Money Laundering Regulations (e.g. external accountants, independent legal advisors, etc); then
- those issued by other organisations.

Banks also perform verification checks on addresses provided by applicants, using data held by multiple public sources as well as internal data records and industry recognised providers. For business entities, this includes the address of the registered office and, if different, the principal business address. Examples of these data sources include:

- Companies House;
- Equifax and Experian data;
- Electoral roll; and
- Other open source data.

The banking and finance sector go beyond standard 'know-your-customer' checks and apply a layered approach to counter fraud. Adverse media, sanctions, fraud screening and anti-impersonation measures are examples of additional checks performed.

There are several industry tools and screening lists used as part of this layered approach; examples include:

- The National Hunter anti-fraud database;
- National SIRA fraud detection and prevention database; and
- CIFAS – the UK Fraud Prevention Service.

Where customers are assessed as being higher risk, enhanced due diligence is undertaken. This includes an assessment of all the risks presented by the person or people who are associated with the account or company. Where required this will be completed through verifying information with the help of documentation and open-source research. This might include:

- Documented and validated Source of Funds and Source of Wealth;
- Validated Nature of Business;
- Certified group structure;
- Copies of trusted documents such as Articles of Association; and

- Copies of accounts.

Banks also monitor accounts after opening, to identify unusual activity and investigate indications of suspicious activity. Identified cases of false applications and other fraudulent conduct are shared across the industry through industry tools and screening lists. This includes cases where banks' risk-based controls fail to prevent fraudulent account opening but subsequently identify anomalies for investigation and confirmation of fraudulent conduct.

Banks also alert law enforcement to potential instances of money laundering or terrorist financing through Suspicious Activity Reports (SARs), making 432,316 SARs between April 2019 and March 2020[3].

I hope this provides further context to our oral evidence on the work of the banking sector in protecting our customers from fraud. If it would be helpful to your work, UK Finance would be happy to provide further in-person briefing to the Select Committee's researchers.

Yours sincerely,

Nick van Benschoten
Director, International Illicit Finance

[3] https://www.nationalcrimeagency.gov.uk/who-we-are/publications/480-sars-annual-report-2020/file