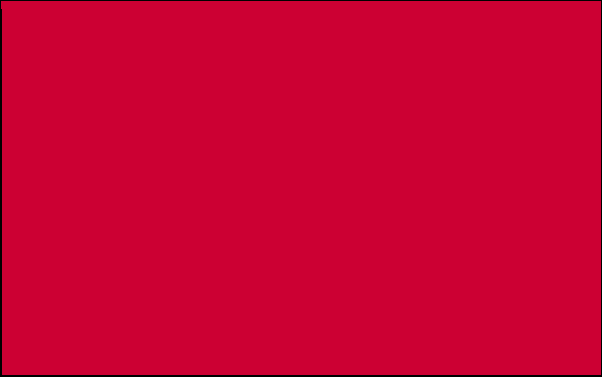


Your response

Question	Your response
Question 1: Do you have any comments on the suggested measures set out in Section 3?	<p>We support measures to ensure operators take a robust risk-based approach to “know you customer” checks.</p> <p>Such checks, especially those of a basic nature, are not necessarily difficult to circumvent. Corporate identity theft is a significant risk that is not necessarily eliminated through reference to Companies House or existing telephony services and websites.</p> <p>It is relatively easy for a potential threat actor to impersonate a perspective customer, using a similar or copycat domain and the provision of a geographic virtual telephony service which appears to match the location of the company in question.</p> <p>As the UK move towards the use of authentication technologies within digital voice, there will be an increase incentive for scam callers to obtain services using corporate identity theft.</p>
Question 2: Have you used any other due diligence checks that you think would be beneficial if adopted across the industry?	<p>We would recommend the use of technology to reduce friction, credit risk and increase confidence. Particularly in those circumstances where the principal sales channel is remote (phone or ecommerce).</p> <p>Operators may wish to utilise technologies such as Open Banking to confirm the identity of a perspective customer by matching the trading style offered to that which is held by the financial institution. This approach will also provide operators with the opportunity to better manage credit risk.</p> <p>The cost of taking this approach should not be significant with several providers offering solutions that require no integration with legacy systems.</p> <p>Solutions such as device identification solutions should also be considered, especially those that provide a reputational score beyond the</p>

	<p>telecommunications industry. Enabling threat actors who are seeking to exploit the ecommerce channels of multiple industry verticals to be excluded.</p>
<p>Question 3: Do you have any comments on the suggested measures set out in Section 4?</p>	<p>None, other than to observe that a continuous approach to the management of risk is essential. Especially in situations where external factors such as business failure can lead to previously low risk customers becoming high risk.</p> <p>In other sectors the execution of fraud using long-firm and short-firm techniques is commonplace. Leading to credit risk and in many cases the misuse of services or assets obtained using a credit facility.</p> <p>Criminal Taxi's are a good example of such tactics, with the offenders operating a clean business in order to obtain vehicle leases. These are then insured ostensibly for the legitimate business purpose before being hired out to criminals who wish to travel in apparently "clean" vehicles.</p>
<p>Question 4: Have you used any other ongoing checks to ensure compliance that you think would be beneficial if adopted across the industry?</p>	<p>Operators could consider the use of Cifas to identify trading styles and directors who have been implicated in short-firm/long-firm fraud.</p> <p>Credit risk should be continuously monitored alongside the customers use of the provided services. Mitigating the risk of "Bust-out fraud" events in which an apparently low risk customer seeks to misuse services.</p>
<p>Question 5: Do you have any comments on the suggested measures set out in Section 5?</p>	<p>Consideration should be given to the potential role for the UK to adopt the approach taken by USTelecom in forming the Industry Traceback Group (ITG).</p> <p>Providing a single process by which misuse can be captured, traced and managed by the industry. Such an approach would also streamline reporting from third parties such as key law enforcement and industry verticals such as financial institutions.</p> <p>A solution of this kind would also facilitate the creation of "trusted flagger" programmes akin</p>



to those offered by Meta and Google. Offering operators a means by which they can have confidence in the assessment process adopted prior to submission.

Additionally, using API's and automated risk scoring there would be scope for the industry to significantly reduce the cost and timeframe for the cessation of misuse.