Your response

Question	Your response
Question 8: Do you agree with our initial views on how to approach key issues for the design and operation of Open Communications? Do you have comments to make on other implementation issues?	Our response focusses on topic of user authentication within the Open Communication framework. We agree that robust and secure processes of authorisation and authentication are critical, and we welcome Ofcom encouraging innovation to enable quick and easy access while maximising security of customer data. With regards to the use of passwords for authentication, there are a number of social and technical vulnerabilities associated with the use of passwords online. Fraudsters are able to exploit these via a number of methods including social engineering, data breaches, brute-force attacks, keyloggers or 'over the shoulder' attacks. Even by mandating unique and/or encrypted passwords, the inherent risks associated with passwords cannot be eliminated. Our research shows that consumers are likely to prioritise convenience and speed of access to online goods and services over security, highlighting the risk of commonly used passwords and/or passwords being stored in an insecure manner. The ICO, while recognising passwords are still commonly used, have highlighted that they carry well-known risks and suggests considering whether better alternatives can be used to provide secure access to services. (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/passwords-in-online-services/) Multi-factor authentication and in particular, the analysis of a user's behaviour, device and location can deliver significantly higher levels of security than passwords. Behaviour can be collected passively while a user inputs data or interacts with a device through the analysis of keystrokes and mouse movements, without adding friction to the journey. Alternatively, users can easily authenticate themselves through new methods such as Swipe (gesturing to provide a non-repudiable digital signature). Across a number of sectors, we are seeing a movement away from the reliance on passwords to these more secure and user-friendly authentication methods. Within Financial Services, for example, the Financial Conduct Authority is supporting the industry's recommendation to use behavioural biometrics, an 'inherence factor', in place of a 'knowledge factor' for online payment authentication as part of PSD2's Strong Customer Authentication (SCA) requirements. (https://www.ukfinance.org.uk/system/files/Strong%20Customer%20Authentication%20-%20Considerations%20for%20what%20can%20be%20used%20as%20a%20second%20factor%20alongside%20One%20Time%20Passcode%20%28OTP%29_0.pdf)

	The European Banking Authority (EBA) has also recognised the potential of inherence for authentication, stating that of the different authentication factors (inherence, knowledge and possession), inherence is the most innovative and fastest moving. Identifying a user by the way they type and swipe, and the angle at which they hold a device was highlighted by the EBA in June 2019 as a compliant way to achieve inherence for SCA. (https://eba.europa.eu/sites/default/documents/files/documents/10180/2622242/4bf4e536-69a5-44a5-a685-de42e292ef78/EBA%20Opinion%20on%20SCA%20elements%20under%20PSD2%20.pdf?retry=1) In addition, we recognise the need for all users to be able to easily access Open Communication services regardless of their circumstances. It is essential to avoid isolating any segments of society, for example those without internet access, those with a disability, or vulnerable customers. The best authentication solutions offer customers a variety of authentication methods, for example using a landline for voice authentication or through facial recognition, to offer the right journey for each individual. There could also be consideration given to the use of digital identity services in the development of Open Communications. There are a number of digital identity initiatives currently underway across both public and private sector, at different stages of development. The ambition for these services is that users benefit from low friction, more consistent and more secure online interactions, without the need for multiple online registrations. This is something we would be happy to discuss and explore further with Ofcom. We would support an innovative approach being taken that ensures the authentication mechanisms for Open Communications provide security alongside positive user experience.