Your response

Question	Your response
Question 1: Do you agree with our proposed guidance on scope? If not, please provide any information or evidence in support of your views, including descriptions of services or content where you consider it is unclear whether they fall within the scope of Part 5.	Confidential? – Y / N
Question 2: Do you have any comments on how our proposed guidance applies in respect of pornographic content created by generative-AI services within the scope of Part 5? Please provide any information or evidence in support of your views.	Confidential? – Y / N
Question 3: Do you have any comments on our proposed guidance in respect of the kinds of age assurance which could be highly effective? If you consider there are other kinds of age assurance which have not been listed that you consider could fulfil the proposed criteria, please identify these with any supporting information or evidence.	GeoComply supports Ofcom in its assessment of age assurance methods that could be highly effective, including photo-ID matching and credit cards. As an age-verification supplier to North America's regulated online gambling and sports wagering industry, GeoComply has a record of preventing underage access to age-restricted products through reliable and accurate verification methods. Effective age verification methods GeoComply focuses on as part of this consultation response are: • Credit cards: verifying personal information, such as name, date of birth, email address or national insurance number, against credit bureau databases. • Photo-ID matching: verifying live biometric data against that found in national identification documents, such as a passport or driver's license. **3.1 Credit Cards:** Verifying an individual's personal information against credit bureau databases is a low-friction and effective method to verify age. Based on GeoComply's experience as a compliance service provider in

Question	Your response
	North America to age-restricted products, key data points to verify age in this way include name, date of birth, email address and social security number (or equivalent). GeoComply delivers such checks in a 'waterfall' process, whereby users' personal information is checked against multiple databases until a successful verification is achieved, increasing the likelihood of a pass without compromising accuracy and integrity. **3.2 Photo-ID Matching:** Photo-ID matching requires an individual to provide biometric information, such as a photo or video. The 'live' biometric information is then cross-referenced against a scan/photo of a national identity document, such as a passport or driver's license. The age is verified when there is a match between the biometrics requested from the user and those provided in the identity document. The effectiveness of such solutions in preventing children from accessing age-restricted products diverges significantly from the less effective methods outlined by Ofcom in the consultation, such as self-declaration. Self-declaration is an ineffective verification method in preventing underage access, putting platforms at risk of hosting child sexual abuse material and causing harm to minors. Therefore, distinguishing between specific age verification methods is essential to meet Ofcom's regulatory expectations.
Question 4: Do you agree that service providers should use the proposed criteria to determine whether the age assurance they implement which is highly effective at correctly determining whether or not a user is a child? Please provide any information or evidence in support of your views.	Confidential? – Y / N

Question	Your response
Question 5: Do you have any information or evidence on the extent of circumvention risk affecting different age assurance methods and/or on any steps that providers might take to manage different circumvention risks for different methods?	**5.1 Risk Identification:** Despite the robustness of photo-ID matching and credit cards as age-verification measures, platforms that host age-restricted products or services should consider how fraudsters, children, or others might circumvent the verification measures. For example, an underground website was recently found to generate realistic-looking photos of fake IDs, such as California driver's licenses, for only $15 online. Moreover, platforms should consider how increasing generative AI technology and 'deep-fakes' adoption might impact such checks. Finally, it should also be considered that an individual might use someone else's personal information to create and log into an account, either obtained through proximity (i.e. an adult or peer) or obtained on the internet (i.e. as a result of various data breaches in personally identifiable information). **5.2 Risk Mitigation:** Fraud tools are only as good as the risk management frameworks in which they are deployed. Platforms can balance security with user access by establishing the correct and appropriate thresholds for suspicious user activity. Thresholds should be set and adapted through continuous and ongoing evidence and research. GeoComply advocates combining multiple checks and data sources to overcome circumvention risks as part of a broader identity authentication and risk management process. This process puts platforms in a more advantageous position to mitigate the disadvantages of each anti-fraud technique. Consequently, platforms can generate a holistic view of typical and predicted user behaviour, enabling more effective identification of anomalies and suspicious account activity. To support our response, GeoComply will discuss two additional identity authentication methods that support holistic risk management on online platforms to overcome circumvention attempts: • Device fingerprinting: a technique used to identify and flag devices on the internet. • Advanced geolocation: collecting and triangulating multiple, device-based geolocation

Question	Your response
	data points, such as GPS, Wi-Fi and GSM data. GeoComply leverages advanced geolocation and device fingerprinting, among other fraud detection techniques, to identify, flag and prevent fraudulent activity in real-time. Our response demonstrates effective Know Your Customer protocols, leveraging multiple authentication techniques to mitigate circumvention attempts. **5.2.1 Device Fingerprinting** Device fingerprinting, or Fingerprinting-as-a-Service (FaaS), is a technique used to identify and flag devices on the internet. FaaS is commonly used as a means to fight fraud and authenticate identity. To create a unique device 'fingerprint, ' information about a device's hardware and software configuration, such as operating system, browser, IP address, screen resolution, etc., is collected. Hardware and software indicators that might make up a device fingerprint vary between service providers, of which there are many in the market. For example, leveraging device fingerprinting as part of a risk management and identity authentication framework enables platforms to establish devices from which accounts are accessed. If a new device attempts to access an account, dependent on risk appetite and regulatory obligations, an online platform may ask the user for additional information to enable them to access that account, such as two-factor authentication. This process ensures that the individual accessing the account is who they say they are and that they are of legal age to consume the content based on prior age verification. **5.2.2 Advanced geolocation** Multi-sourced geolocation data points, such as GPS, Wi-Fi Triangulation and GSM, enhance authentication processes by strengthening a platform's ability to identify anomalous user behaviour. Such data provides far more accurate and reliable location data sources than an IP address. Shortcomings associated with using IP for location include (but are not limited to): • The mainstream use of VPNs and proxies on the internet, which alter an IP address;

Question	Your response
	• The growing use of relay proxies (such as Apple Relay or Google One), which are built into devices that billions of people use daily; • Dynamic IP addresses (i.e. those associated with mobile devices) do not indicate device location, often resolving back to carrier location; • Based on GeoComply data, the approximate range of an IP address is 100km. Consequently, we strongly recommend **against** relying upon an IP address to block/prevent users from reentering a service. Instead, by leveraging multiple geolocation data sources, such as GPS, Wi-Fi Triangulation, and GSM, a platform can cross-reference data points and ensure higher accuracy in locating an individual or device. Furthermore, by leveraging geolocation in authentication, platforms could identify and manage suspicious locations and hotspots for illegal activity. For example, geolocation would enable platforms to flag frequent log-in attempts from schools, which could trigger further action or investigation. As a non-biased, privacy-preserving strategy to ensure internet safety and strengthen authentication processes, multi-source geolocation and device data are critical for fraud and suspicious activity detection. These data points enhance a user's risk profile without compromising their natural identity.
Question 6: Do you agree with our proposed guidance that providers should consider accessibility and interoperability when implementing age assurance? Please provide any information or evidence in support of your views.	Confidential? – Y / N
Question 7: Do you have comments on the illustrative case study we have set out in the guidance? Do you have any supporting information or evidence relating to additional examples of how the criteria and principles might apply to different age assurance processes?	Confidential? – Y / N

Question	Your response
Question 8: Do you agree with our proposed guidance on the record-keeping duties? Please provide any information or evidence in support of your views.	Confidential? – Y / N
Question 9: Do you have any comments on our proposed approach to assessing compliance with the duties on service providers who publish or display pornographic content, including on the proposed examples of non-compliance? Please provide any information or evidence in support of your views.	Confidential? – Y / N
Question 10: Do you have any comments on the impact assessment set out in Annex 1? Please provide any information or evidence in support of your views	Confidential? – Y / N
Question 11: Do you agree that our proposed guidance is likely to have positive effects on opportunities to use Welsh and treating Welsh no less favourably than English? If you disagree, please explain why, including how you consider the proposed guidance could be revised to have positive effects or more positive effects, or no adverse effects or fewer adverse effects on opportunities to use Welsh and treating Welsh no less favourably than English.	Confidential? – Y / N

Please complete this form in full and return to Part5Guidance@ofcom.org.uk.