WHITE PAPER

WHO IS ONLINE?

VERIFYING IDENTITY IN SUPPORT OF THE ONLINE SAFETY ACT.

CONTENTS

Executive Summary	3 - 4
Ofcom ranks open banking highly for age assurance.	5 - 6
Background to the Online Safety Act	7 - 8
New regulatory regime for online safety	9
How does age verification work today?	10
How can bank-verified digital data sharing provide age assurance?	11 - 14
About OneID®	15

EXECUTIVE SUMMARY:

THE ONLINE SAFETY ACT – NOW A LAW

The UK's long-awaited Online Safety Act, which sets tougher content moderation standards, has finally become law. Internet firms and social media platforms like Facebook, YouTube and TikTok will be required to remove "illegal content" quickly or prevent it from appearing in the first place.

They will also need to use age-verification technology to ensure that their users are over 18 years old to protect children from being exposed to "content that is harmful to children".

WHAT CONSTITUTES ILLEGAL CONTENT?

"Illegal content" covers content relating to terrorism, child abuse material, and fraud; things that are illegal to present to anyone.

"Content that is harmful to children" is split into three categories:

"Primary priority content"

- Pornography
- Suicide
- Self-injury
- Eating disorders

"Priority content"

- Abusive content relating to race, religion, sex, sexual orientation or disability
- Violent or bullying content against people or animals (that doesn't need to be real)
- Dangerous challenges, ingesting substances

"Non-designated content"

- Anything not defined in the other two categories that could cause harm to children

SAFETY – WITHOUT COMPROMISING ON USER EXPERIENCE

Firms in the scope of the Online Safety Act will need to verify the age of their users in a frictionless yet accurate way, without damaging user experience, to ensure that they don't present harmful content to children.

This paper explores how bank-verified digital identity and age verification solutions can enable UK adults to verify their age easily and protect minors from age-restricted and harmful content. All this while helping online platforms avoid significant fines for breaching the new Online Safety Act.

ABSOLUTE CERTAINTY WITH BANK-VERIFIED DIGITAL IDENTITY VERIFICATION

Unlike many other forms of attribute verification, a bank-verified data solution is highly flexible. It can be instantly tailored to provide proof of age specifically while withholding other personal information such as name and address.

Hence, this approach can preserve a user's anonymity, where appropriate, which mitigates any concerns that the Online Safety Act will create a form of state-sponsored surveillance of citizens' online activities, likes and dislikes.

ONEID® – THE FASTEST AND EASIEST WAY TO VERIFY PEOPLE ARE WHO THEY SAY THEY ARE

At OneID®, we welcome the Online Safety Act and stand ready to support the regulators and online platforms in rolling out a safe and cost-effective solution to verify the age of their users.

OneID® is a UK-based fintech that is the only provider of truly digital, real-time identity and age verification services in the fastest, cheapest, and safest way. It is the only UK Identity Service with access to bank-verified data to ensure that the most advanced counter-fraud measures protect every transaction.

OFCOM RANKS OPEN BANKING HIGHLY FOR AGE ASSURANCE.

In preparation for the Online Safety Act last year the UK Information Commissioner's Office (ICO) requested that the Age Check Certification Scheme (ACCS) should produce a technical study about the measurement of age assurance technologies. Subsequently, in conjunction with Ofcom, the ICO commissioned a detailed technical study into the accuracy of various age assurance methods offered by solution providers, including combined approaches, alongside an assessment of current effectiveness and anticipated effectiveness over the next five years.

The ACCS' research focussed on eight age assurance techniques selected. Five of these were "age verification" measures:

- Electoral registration or credit reference
- Mobile telephone content control measures
- Credit card holder check
- Passport / driving licence ID scan
- Connections to bank account information

Three of these were "age estimation" measures:

- Facial analysis age estimation
- Voice age estimation
- Usage of an e-mail address over time as a method of age estimation

The ACCS research concluded that of these eight forms of age assurance, only two achieve the highest level of Strict Accuracy **(99.99%)**. The first of these is the traditional but manually intensive method of using a passport or driving license to demonstrate a person's age by scanning or taking a photo of the document and uploading it to the party trying to verify your age. The second and less well-known method is what the ACCS call Open Banking Connect. This refers to an age assurance solution provider which uses connections to bank information to automate this process.

Strikingly, the ACCs highlights that there were twelve age assurance providers out of the total pool of research participants which use scanned passports and / or driving licenses to verify ages as either one element of or their entire age checking process. Furthermore, only four of these solution providers are currently certified for this activity. On the other hand, there is only one age assurance provider which uses connections to bank information to deliver this service and it is fully certified.

OneID® is certified by the ACCS for its ability to safeguard young people by preventing access to age-restricted products and services, making this solution the clear leader for enabling internet firms to comply with the Online Safety Act.

[1]The Age Check Certification Scheme (ACCS) is an independent third-party conformity assessment service operated by AVID Certification Services Ltd and accredited by the United Kingdom Accreditation Service (UKAS). The scheme is established to undertake standards-based assessments of age assurance es, digital identity services and age-appropriate design of information society services. They check that ID and age check systems work.

[2]Measurement of Age Assurance Technologies Part 2 – Current and short-term capability of a range of Age Assurance measures, The Age Checking Certification Scheme, 2023

BACKGROUND TO THE ONLINE SAFETY ACT

In a world now dominated by social media and the internet, online platforms have long been criticised for not doing enough to tackle illegal and harmful content on their platforms.
Easy access to damaging material, particularly for young people, came into the spotlight after the death of 14-year-old Molly Russell in 2017, which her parents said came after she had viewed online material on depression and suicide.
That same year, the government published an Internet Safety Strategy, which eventually became the Online Harms Bill, later renamed the Online Safety Bill.

Free speech remains at the heart of any open and democratic society. But with the exponential evolution of the digital landscape, new forms of harm such as cyber-bullying, hate speech, revenge porn and child exploitation have emerged. The UK government's Online Safety Data Initiative, launched in September 2021, stated:

"The internet can be a powerful force for good, but illegal and harmful content and activity is widespread online.

62% of adult internet users and over 80% of children (aged 12-15) have had potentially harmful experiences online."

The Online Safety Act addresses these issues by imposing legal obligations on social media firms and other online platforms to protect users from being exposed to illegal and harmful content.
The Act affects social media platforms that host user-generated content, like X (formerly known as Twitter), Facebook and TikTok, and search engines such as Google. The new act also impacts other smaller sites which enable user-to-user sharing.

According to the government, the Online Safety Act puts into law "rules to make the UK the safest place in the world to be online" by placing world-first legal duties on social media platforms.

SCOPE OF THE ONLINE SAFETY ACT

The new act addresses a range of issues to establish a safer online environment on social media sites, such as minimising fraudulent advertisements, tightening laws on illegal content, ensuring harmful content is not accessible by children, and even giving adult users more control over the content they are exposed to.

The Online Safety Act requires internet firms, such as social media platforms, to remove all illegal content, such as terrorism and child abuse related content. It also brings in new offences; for example, content which promotes self-harm or suicide cannot be shown to children.

Platforms need to have continuous risk assessment relating to illegal content, while written records of such assessments must be kept and updated with proactive steps to mitigate and manage risks of harm to individuals caused by illegal content as identified in their risk assessments.

There is a requirement for platforms to establish adequate systems and processes to protect user safety. Platforms are obliged to offer processes for users to report illegal content, as well as harmful material, and they are required to operate accessible complaint procedures for users.

CONTENT THAT IS HARMFUL TO CHILDREN

Not all harmful content which appears online is actually illegal. For example, although it is not considered to be a criminal offence to promote or glorify an eating disorder, such activity could be detrimental to a young person's wellbeing. The Online Safety Act, therefore requires social media platforms to put in place more stringent measures to prevent children or young people from being exposed to this kind of material. Internet firms are, therefore required to use age-verification services to ensure that children are not exposed to harmful content. This refers to content which is not against the law but could be seen to encourage abuse or trauma.

Age-checking procedures, age limitations, and provisions for parents/guardians to report problems online and provide them with tools to give more control over the type of content accessed by their children are just some of the measures the Online Safety Act proposes.

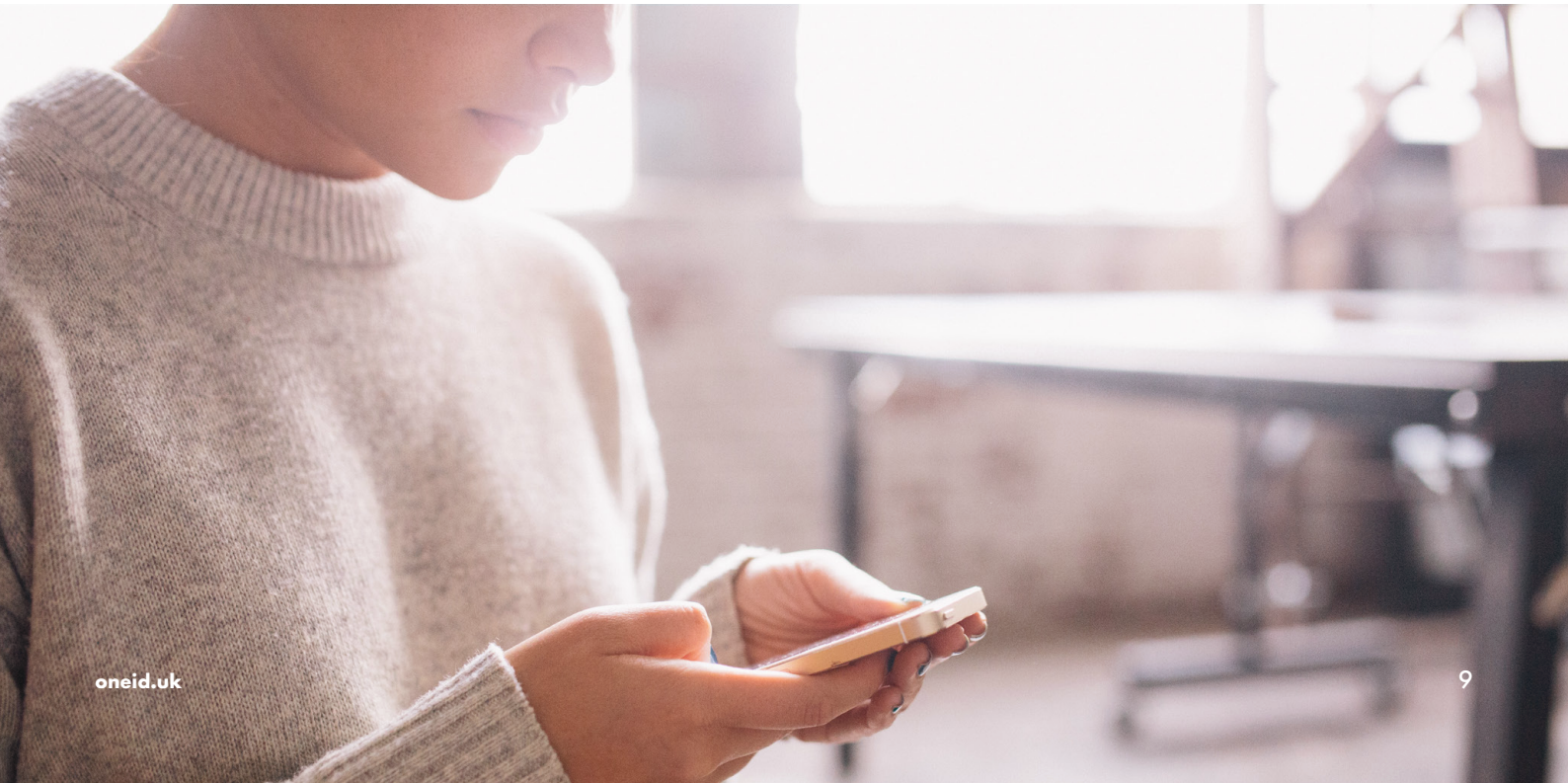
Internet firms must also publish a summary of their risk assessments concerning the dangers posed to children and give Ofcom the power to publish details of any enforcement action it takes. The intent is to safeguard young people, stamp out criminality, and give adults control over what they see and engage with online.

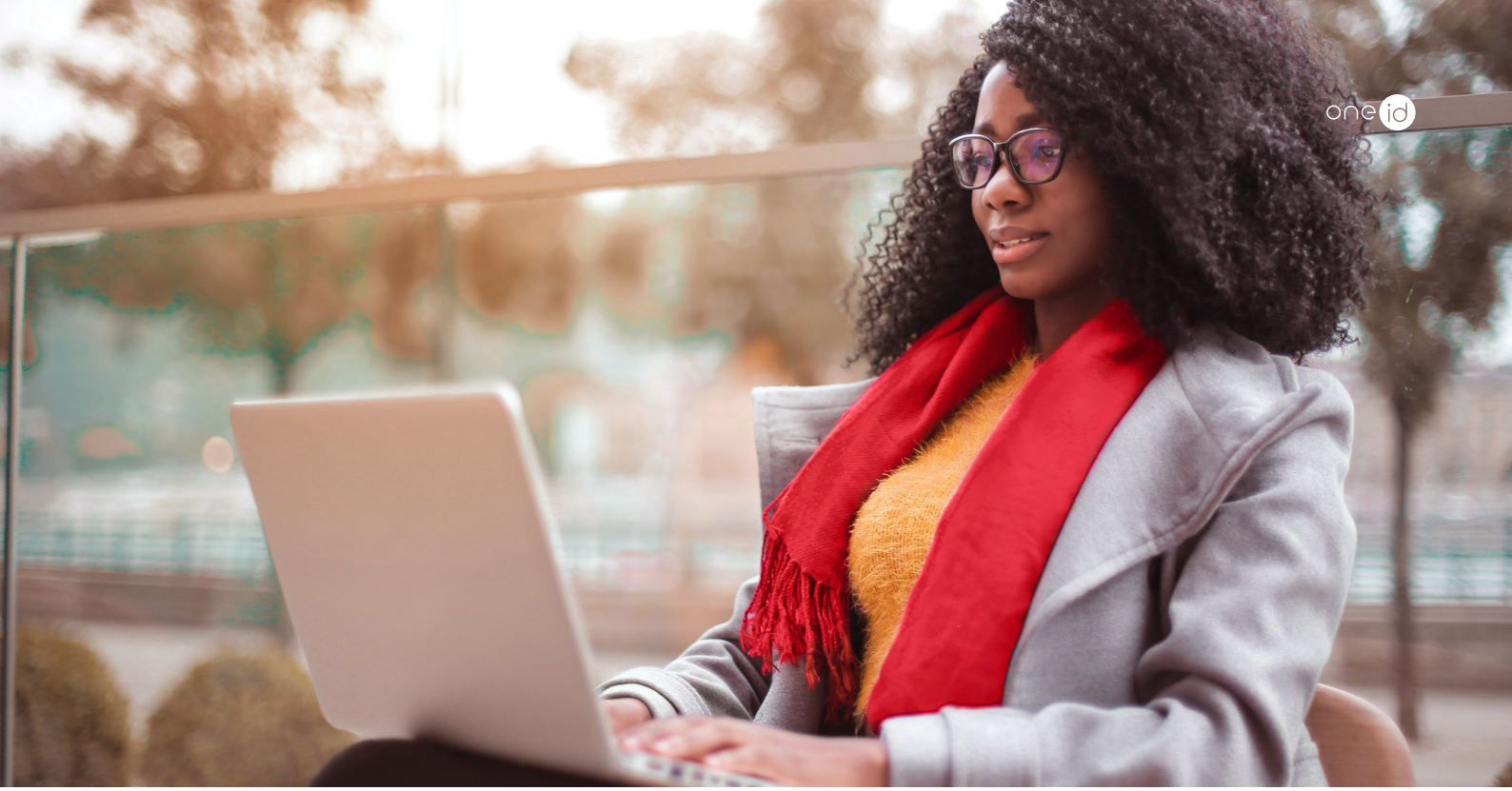
Platforms also need to include features to give adults more control over what content they view online so that they can reduce their likelihood of viewing harmful content or receiving an alert from the service as to the harmful nature of the content.

NEW REGULATORY REGIME FOR ONLINE SAFETY

Ofcom is in charge of implementing and overseeing the new regulatory regime and industry engagement. They are granted powers of enforcement to take action against non-complying platforms. Internet firms that fail to comply will be fined up to **£18 million** or **10%** of their annual turnover. In the most severe cases, firms could also be banned from operating in the UK if they do not do everything reasonably practical to eradicate harmful content. Ofcom will also require internet firms to publish annual transparency reports and have clear and accessible terms of service that state how users are to be protected from illegal and harmful content.

Ofcom is gearing up its technical and human resources to regulate online safety, recruiting over 300 staff. In April 2023, the regulator launched a new Online Safety Group, which benefits from a wide range of expertise, including people who worked at the biggest tech companies and experts in specific harms. Ofcom is publishing three phases of consultations and draft codes of practice. Phase one focuses on illegal content duties and will set out measures regulated services can take to mitigate the risk of harm caused by illegal content. Phase two will focus on child protection duties, including online pornography. Finally, phase three will cover transparency, user empowerment, and other duties on categorised platforms.





HOW DOES AGE VERIFICATION WORK TODAY?

Age and identity verification are essential to customer onboarding processes in numerous industries and scenarios. Today, individuals are asked to upload a photo of their passport or driving license. However, this method causes considerable friction in the account setup process, can be error-prone, time-consuming and feels outdated.

Digital natives do not want to be troubled by analogue processes like this, even those partly digitised through techniques like scanning physical documents.

These burdensome and repetitive onboarding processes for age and identity verification can be strengthened and streamlined by a combination of new technology and the tried and tested Know Your Customer (KYC) discipline already applied by commercial banks. These new solutions are already beginning to help regulated entities reduce the cost and complexity of anti-money laundering (AML) compliance, mitigating the risk of fines and other reputational damage while reducing the risk of fraud and delivering an inclusive and enhanced customer experience.

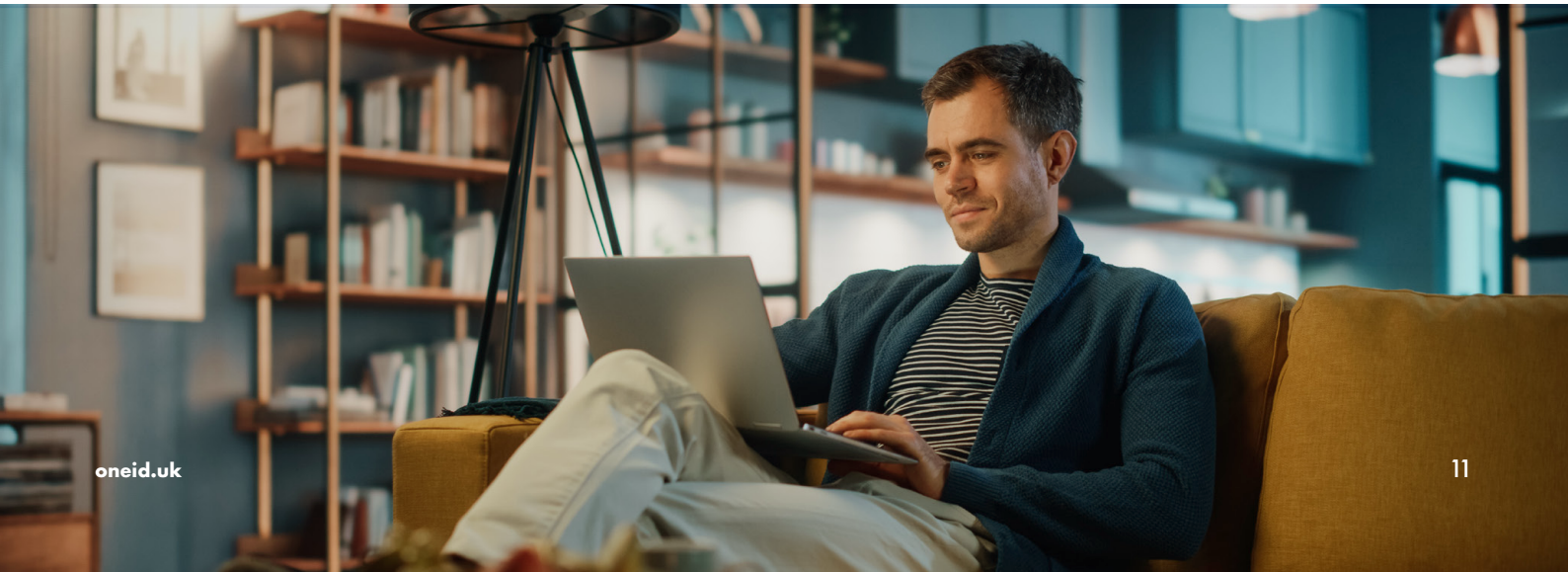
HOW CAN BANK-VERIFIED DIGITAL DATA SHARING PROVIDE AGE ASSURANCE?

A second-generation reusable digital identity and age verification solution is now available in the UK which leverages the robust identity checks that banks perform on their customers. Bank-verified digital identity verification is widely used in other countries such as Canada and the Nordics to successfully reduce fraud and streamline customer on-boarding.

A similar solution can now be used in the UK to verify individuals in a few seconds, making it a low friction process. Bank-verified digital identity and age verification is faster and easier for all people who use internet or mobile banking, allowing them to quickly and securely demonstrate that they are over 18 years old.

Bank-verified digital identity and age verification services are highly flexible. Different data sets can be shared with an internet firm and any other business or government entity, depending on the type of verification that is required. This could include a person's name, address, date of birth or contact information.

But specifically in the case of compliance with the Online Safety Act, the data to be shared with an internet firm can be limited to "the user is over 18", or any other age gate required by the internet firm. The exact type of data to be shared is completely under the control of the individual who sees and consents to the data being shared by their bank on every occasion.



WHY BANKS PLAY A KEY ROLE

Banks enjoy a strong position of trust since millions trust banks with their savings. Banks are heavily regulated and are required to apply rigorous KYC and AML checks to verify the identity of their customers and ensure they are not criminals, terrorists or money launders.
It is this comprehensive level of checking that banks are ideally placed to support a digital identity and/or age verification service.

Banks are also under constant attack by cyber-criminals, and must maintain a higher IT security spend than any other sector to protect against illicit access to bank accounts.
Banks have a better track record than other industries in protecting their customers' personal data. Digital identity and age verified by banks can be quickly integrated by social media platforms on their customer-facing website using secure technology to make it easier for their customers to digitally verify their age or identity, creating an improved customer experience.

NEW MARKET INFRASTRUCTURE UNDERPINNING BANK-VERIFIED DATA SHARING

Not only has the UK government developed rules and governance for the digital identity landscape by introducing a framework for certification, known as the Digital Identity and Attributes Trust Framework (DIATF). In addition, thanks to Open Banking, UK banks have also developed a market infrastructure which enables individuals to securely authorise their bank to share account data with suitably regulated parties.

The combination of an identity framework and modern bank data-sharing platform has enabled new secure, regulated and certified identity services.

BANK-VERIFIED DATA'S POWERFUL REACH AND EASE OF USE

50 million adults in the UK bank online. That compares favourably with individuals who have a passport or a driving license.

Using a bank account as the source of identity and age verification therefore covers a greater percentage of the UK adult population and is more inclusive as more citizens have a bank account.

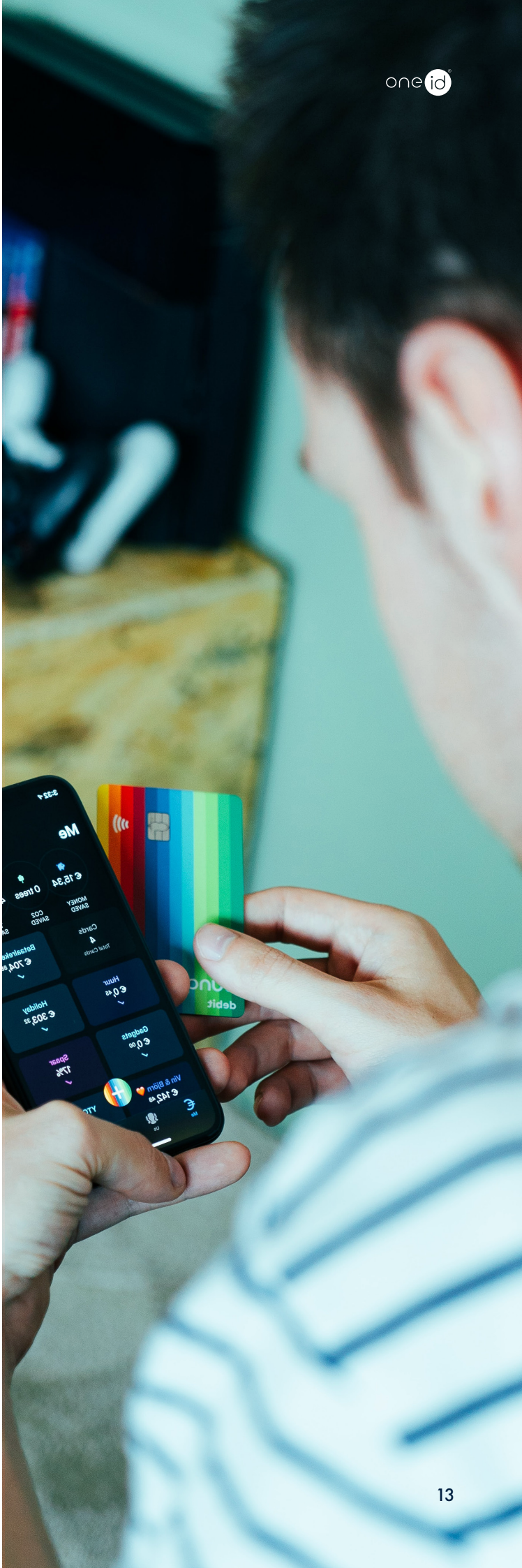
In the context of the Online Safety Act, internet firms can enable prospective and existing users to quickly provide consent to their bank to verify their age or full identity, with just a few clicks and in real time. Consumers do not need to download an app, nor upload documents or photos to a new website. Instead, they simply use their banking app to consent to their bank sharing the required data with any specified organisation, such as a social media platform which has activated this service.

Bank-verified data is therefore more convenient for UK citizens, without the need for cumbersome paperwork. This convenience not only enhances user experience but also boosts customer satisfaction and loyalty, improving overall customer retention rates.

HOW BANK-VERIFIED DATA SHARING WORKS IN PRACTICE

Bank-verified data eliminates the need for an individual to type in their details or upload documents and selfies. All that an individual has to do is click on the data-sharing solution button on the social media platform. This button leads to a menu of bank logos. On selecting the bank logo where the individual holds their main bank account, they are taken to their banking app and use their normal, secure banking credentials to give consent to their bank to provide the platform with the required but tailored personal details, such as age confirmation.

This data is transferred securely and in real-time to the relying party's platform to provide authentication of the individual's age or identity as required. This reduces the need to key in their details and the chance of error. The same process can be used when regularly logging into a website, avoiding the need for additional logins and passwords. A bank-verified digital data verification process is faster and easier because it doe not need any document or selfie uploads. It's also more secure because documents and selfies can be faked in the age of AI. The loss ultimately is borne by the business – in the form of losing customers to clunky experiences, or in the form of fines for non-compliance.



BANK-BASED DATA FOR AGE VERIFICATION ENABLES COMPLIANCE WITH THE ONLINE SAFETY ACT AGE ASSURANCE CHECKS

The Online Safety Act is arguably the most advanced piece of legislation for protecting internet users and radically changes the liability model for illegal and harmful content. Internet firms, including search engines and social media platforms, are required to remove illegal content quickly and protect users, especially children, from harmful content. They will also have to tighten up their age assurance processes to ensure that children are protected from illegal or harmful content. But they will have to do it all in a frictionless and easy to use way, to avoid disrupting their business model.

Next generation solutions based on data provided by banks in real time are highly flexible and can be tailored to provide verification of an online user's actual age or simply to confirm that they are "over 18", as required by the social media platform for particular types of age-related content. More detailed personal information such as name, address and contact details can also be shared, but always under the complete control of the individual wanting to share their data.

This innovative solution set is ideally placed to provide a state-of-the-art age verification solution to help internet firms enable their users to demonstrate that they are over 18 in a frictionless yet highly accurate way, so they can access adult content if they wish to do so. This in turn will make it faster, easier and more cost effective than other age assurance solutions to comply with the Online Safety Act to protect children from inappropriate material, such as adult content or potentially harmful subjects.

Authored by:

Paula Sussex, CEO, OneID®
Adrian Field, Director of Market Development, OneID®

ONEID® – BRINGING EASE TO AGE COMPLIANCE

OneID® is the only provider of truly digital, real-time identity and age verification services that create absolute certainty between a business and a customer in the fastest, cheapest and safest way. It is the only UK Identity Service with access to bank-verified data to ensure that the most advanced counter-fraud measures protect every transaction.

OneID® helps protect banks, businesses, and consumers from online identity fraud. Streamlining existing processes that require identity verification, including payments, direct debits, customer onboarding, and more, OneID® enables businesses to reduce operational costs, increase sales, and improve customer engagement.

CERTIFICATIONS

OneID® is certified by the Age Check Certification Scheme (ACCS), which safeguards young people by preventing access to age-restricted products and services.

OneID® is certified as a Digital Identity Service Provider, authorised by HM Government's Department for Science, Innovation & Technology (DSIT), under their UK Digital Identity & Attributes Framework (DIATF). We were also the first Orchestration Service Provider to receive certification. This allows OneID® to act as a hub to connect all of the UK's high street banks with providers and any online journey that needs customers to identify themselves.

OneID® is also the first Scheme Owner to be certified under the DIATF for any role. It operates a multi-sector scheme that enables bank customers to consent to share their bank-verified identity information safely. OneID® ensures that all businesses in the scheme have been appropriately vetted and given a OneID® Trustmark so that you know the business you are dealing with is legitimate.

Our certifications also include schemes such as Disclosure & Barring Service (DBS) checks for employee screening and Anti-Money Laundering (AML) compliant identity verification.

REGULATED AND AUTHORISED

OneID® is also regulated by the Financial Conduct Authority (FCA) to act as an Account Information Service Provider (AISP) under the Payment Services Regulations, 2017. This means OneID® is authorised, with customer consent, to use Open Banking infrastructure to capture personal data from banks and share this with selected parties in real-time.

About OneID®

OneID® is the only provider of truly digital, real-time identity services that create absolute certainty between a business and a customer, in the fastest, cheapest and safest way.

Our digital ID services use the most advanced counter-fraud measures to help protect banks, businesses and consumers from online identity fraud. By streamlining existing ID processes, including payments, direct debits, onboarding and more, we help businesses reduce operational costs, increase sales and improve customer engagement. As the only UK Identity Service with access to bank-verified data, nearly 50 million UK adults are already set up to use OneID®, for real-time verification.

OneID® is government certified, regulated by the FCA and is a BCorp business.

Headquartered in the UK, we have brought together the best people in Digital Identity, Payments, Banking, Technology and Government to ensure we make the world a safer place.

To learn more visit **www.oneid.uk**.

FOR MORE INFORMATION
Contact Keith Mabbitt,
07790 494 836