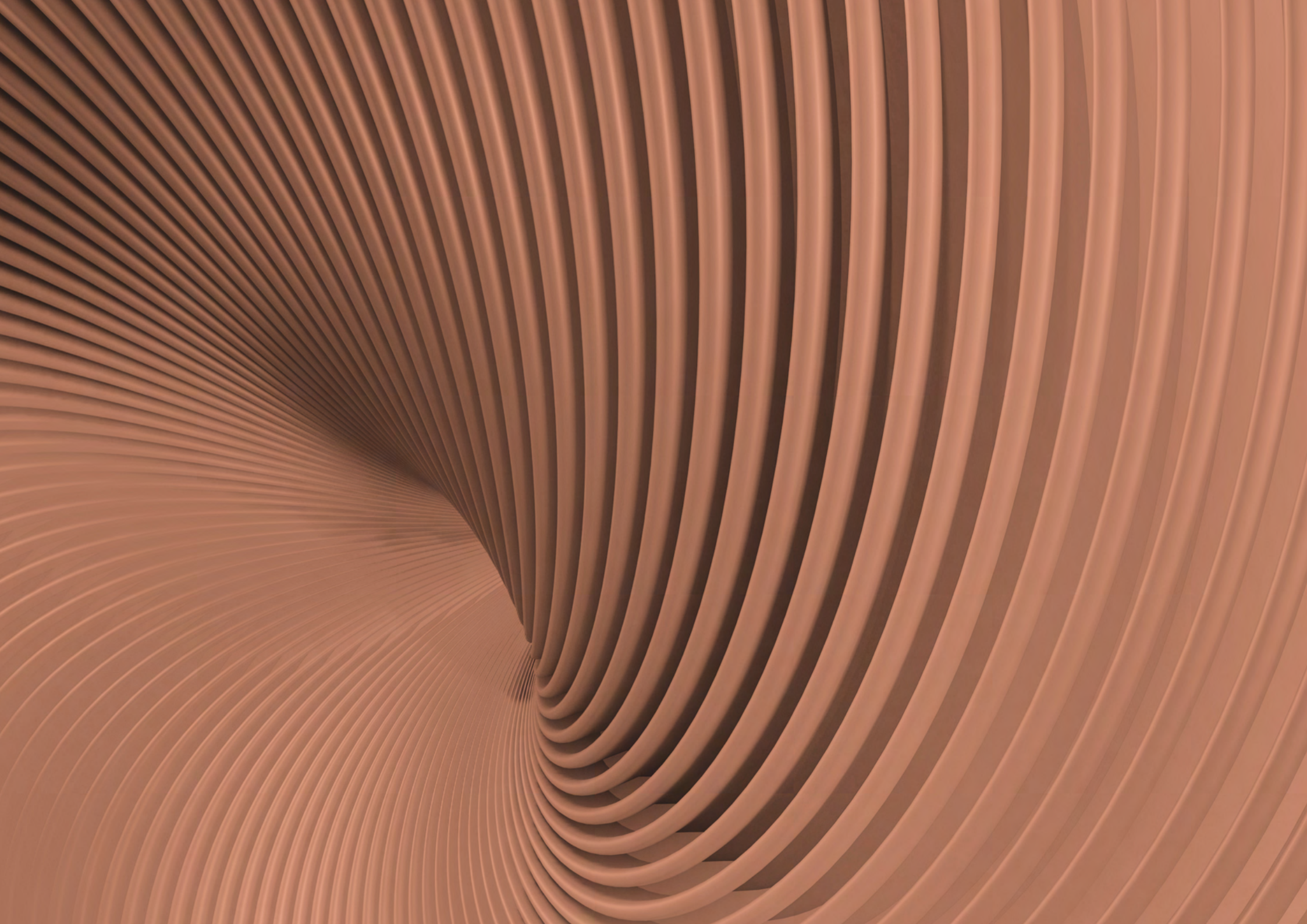


LAWTECH 

Regulatory Response Unit

**Joint Statement
in support of digital
identity technology
in the legal sector**

TECH 
NATION



Joint Statement in support of digital identity technology in the legal sector

Purpose

LawtechUK and the Regulatory Response Unit (RRU) have issued this joint statement to help address misconceptions around digital identity (or 'ID') verification technology, highlight the benefits of adoption in this area, and share useful resources to help legal practitioners in their adoption of such tools.

When used correctly, digital ID verification can provide a fast, cost-effective, and reliable way to verify an individual's identity and reduce money laundering and compliance risks. It can make it easier to spot fake documents for example, and make the client onboarding process faster and smoother. Use of digital ID verification is recognised by The Legal Sector Affinity Group (LSAG) as being "more secure and sophisticated, and may in fact be lower risk than traditional means".

Despite the many benefits of digital ID verification, LawtechUK and the RRU have identified reluctance within the legal community in adopting technology that enables legal practitioners and businesses to verify the identity of their clients through digital means. This reluctance often stems from misconceptions around regulation, and a lack of awareness around the technical capabilities now available.

Legal services regulation does not prohibit the use of digital ID verification tools in any of the jurisdictions of the UK. Digital ID verification technology is established now, and the Government is working to encourage and unify ID verification across sectors, for the benefit of the public and professionals.

This statement does not constitute legal or regulatory advice, and should not replace specific analysis and consultation regarding individual circumstances.

"We are often approached by practitioners unsure of whether they are able to use digital ID verification tools under the regulations. This statement should provide assurance that, when used correctly, regulators not only accept, but support the use of such technologies."

Paul Mosson,
Executive Director of Member Engagement and Services,
Law Society of Scotland

"We have been struck by the speed with which many CLC-regulated practices were able to adopt digital ID tools in 2020 as they responded to the demands of remote working. Since that time, adoption has slowed despite the benefits in terms of confidence and security."

We hope that this note will address any concerns practices may have about digital ID tech and demonstrate the CLC's support for it."






Stephen Ward,
Director of Strategy and External Relations, CLC



"Our 'Striking the Balance' report outlines the practical steps that regulators can take to foster innovation. This includes engaging with their regulated communities to understand the regulatory barriers, both real and perceived, to the use of technology."

This joint statement is an example of regulators responding to a barrier that they have identified, by seeking to dispel misconceptions around digital ID tools. We look forward to continuing to work with regulators to foster innovation that opens-up access to legal services."

Chris Nichols,
Director of Policy and Regulation, Legal Services Board

Benefits of Digital ID Verification Technology

-  **Confidence**
Digital ID verification can involve a number of technologies, including biometric verification, facial recognition, 'liveness' checks, machine readable zones (MRZ) and others. These can increase the accuracy of checks, while reducing room for human error, enabling legal practitioners to be confident about their client's identity.
-  **Speed**
These tools can save time on manual processing of documentation and in-person checking through remote onboarding and accelerated verification processes.
-  **Scalability**
Once digital ID processes are set up, they can scale easily for use with all clients.
-  **Record Keeping**
Providers may include features such as automated record-keeping that ensure data is captured in a way that is standardised and secure. This can be useful for evaluation and auditing purposes.
-  **Compliance**
Processes and controls correctly implemented with digital ID tools map to legal requirements, reducing the complexity for practitioners to both comply and evidence compliance to regulations.

-  **User experience**
Digital ID tools make the identity verification process less burdensome for the client, from simple instructions on how to upload documents, handling requests for additional information, and communication on status and outcome, which otherwise involve lots of back and forth correspondence e.g. by email.
-  **Security**
Documents can be encrypted and stored digitally and securely. This reduces the risk associated with physical storage and management of documents.

“As the practice of law develops we need to make sure that legal professionals are using the most efficient and effective ways of managing risk. Digital IDs offer, in most cases, a better solution than traditional manual checking. As this paper demonstrates they are encouraged by regulators. There is no reason for legal professionals to avoid their use as a matter of principle. The debate should move onto what is the best system and how it can be implemented.”

Iain Miller,
Partner, Kingsley Napley

“We see that the law firms that use digital ID technology (and alongside it, ongoing risk monitoring and other top in class AML tools), have driven far more certainty and effectiveness in their AML compliance operations. Firms have also noted the ancillary benefits – the ability for clients to benefit from the same modern, digital experience that they have come to expect from other industries like banking.”

Julia Salasky,
CEO, Legl

Background

Money laundering and financial fraud are widespread issues. The National Crime Agency estimates that money laundering costs the UK economy £100bn every year.¹ UK Finance revealed push payment fraud losses totalled £479m in 2020, with many more cases anticipated than the 150,000 incidents reported.² These statistics are trending upwards.

Professionals and organisations that hold and handle customer money, such as legal practitioners and law firms, are subject to stringent anti-money laundering and customer due diligence controls, which are evolving frequently. The UK is a target jurisdiction for money laundering, with legal practitioners seen as attractive because of the position of trust they hold. In 2021 alone, the SRA issued fines of £160,000 due to poor AML compliance.³

The legal community faces increasing challenges in meeting and keeping up with the various requirements and many still opt for manual methods of doing so. Given adoption rates of digital ID technology across all sectors, the use of digital ID checking is predicted to become the default in the near-future.

Digital ID tools are already in use as part of day-to-day activities in other sectors. For example in banking apps, vaccine passports, and e-passport gates that combine digital ID technology with biometric scanning to verify identity. This is particularly beneficial where remote alternatives to face-to-face verification have become not only convenient, but necessary during lock down measures.

Manual methods of identity verification involve checking passport details, photographs, proof of address, source of funds, and beneficial

ownership information in person and sharing and storing the paperwork physically. Manual verification may be appropriate in certain circumstances, for example where the client is unable or unwilling to use a digital ID tool or where face to face checks are required in certain jurisdictions. Practitioners should be comfortable using both digital and manual ID verification practises.

“As part of the global fight against money laundering, identity fraud, and terrorism financing, it’s vital that practising lawyers take every necessary step to ensure that the legitimate services provided by legal firms are not misused. Secure, online solutions can greatly reduce the administrative burden on law firms, while ensuring practitioners can continue to meet their legal duties.”

Cutting out hours of paper-based processes involved in crucial compliance checks allows practitioners to focus on what they do best in meeting the legal needs of their clients, while assured that they have robust due diligence systems in place.”

Paul Mosson,
Executive Director of Member Engagement and Services,
Law Society of Scotland

1 - [National Economic Crime Centre leads push to identify money laundering activity - National Crime Agency](#)

2 - [FRAUD - THE FACTS 2021 - UK Finance](#)

3 - <https://www.sra.org.uk/sra/research-report/antimoney-laundering/>

Digital ID in the Legal Sector

Professional Indemnity Insurance (PII)

Insurers are engaging with digital ID technology in quantifying risk and evaluating insurance premiums for law firms. This has been seen with the underwriting agent Inperio's partnership with Thirdfort, which reduces premiums and excesses for firms using Thirdfort digital ID technology.

"It is clear to Inperio that more legal practices need to embrace technology or risk being ostracised by their peers. Digital ID checking is a simple solution, which has huge benefits for consumers and legal practices, both in the speed clients can be onboarded and the material reduction in transactions involving identity fraud. We see a future where digital ID checks are the basic standard practitioners look for when reporting to their clients on counter-party risk."
Simon Lovat, CEO, Inperio

Conveyancing

HM Land Registry will offer a 'safe harbour' to conveyancers using a digital identity method under this standard, meaning the Land Registry will not seek recourse against those who comply with the digital ID standard, even if their client was not who they claimed to be.

"One-quarter of CLC-regulated firms adopted digital ID verification between March and October 2020 to make ID checking and AML compliance more resilient to pandemic circumstances."

"When they began to look at the benefits and approach to implementation, they were able to work quickly. Some firms were already using such tools, but many others have still not engaged with the opportunity and this statement will help." Stephen Ward, Director of Strategy and External Relations, CLC

Obligations

- When acting under the scope of the money laundering regulations, legal practitioners must carry out customer due diligence (CDD) and 'enhanced' due diligence in a range of circumstances, for example when establishing new business relationships, undertaking specific transactions, and when they suspect criminality or doubt veracity. They have to ensure they verify client identity based on a reliable source, identify source of funds and beneficial ownership, and assess and record the purpose and intended nature of the relevant relationship or transaction.⁴
- The Government standard for verifying identities digitally defines four 'Levels of Confidence': low, medium, high and very high. The higher the Level of Confidence, the more trust can be placed in the identity. Digital identity verification provides a 'medium' level of confidence, and is in line with the money laundering regulations.⁵
- Practitioners are increasingly required to mitigate risks relating to identity, push payment and other frauds, such as where payments are intercepted by a criminal third party in a property transaction. For instance, in *P&P Property Ltd v Owen White & Catlin LLP*,⁶ a law firm was held liable for identity fraud in such a transaction.
- Requirements can be met via both manual and digital processes. However, the features and capability associated with each differ significantly, as illustrated below:

4 - [The Money Laundering, Terrorist Financing and Transfer of Funds \(Information on the Payer\) Regulations 2017](#)

5 - [How to prove and verify someone's identity - GOV.UK](#)

6 - [2018] EWCA Civ 1082 (15 May 2018)



Manual



EVIDENCE COLLECTION



Identity documents such as passports or birth certificates are collected in **person or by post**.

Attribute information is copied or recorded and **stored physically**, ideally behind a lock or within a safe. This approach relies on **individual due diligence** for its effectiveness.



DOCUMENT VALIDATION



Document authenticity is validated via **visual examination of physical security features**.

Validation is conducted by human-eye and **may vary in standard** according to training and available tools.

Specialist training is required to identify whether documents presented are fraudulent.



IDENTITY VERIFICATION



Physical and visual comparison is made between the documentation provided and a **face-to face interaction** with the person claiming the presented identity.

Separate teams (eg. compliance, legal, support) within a firm may each need to **individually review** the identity for due diligence purposes.



Digital



Identity information may be **submitted digitally**, and/or collected via an information store and checked against **numerous online databases** in real-time. It is **automatically encrypted** and stored in secure digital form.

The technology also helps to **screen out synthetic identities** used by imposters.



Documents are validated using **cryptographic techniques**, character recognition, digital signature and Machine Readable Zone (MRZ) checks of multiple document security features.

Validation through the tool is **consistent in accuracy**, with attributes and data points **automatically corroborated in real-time** against numerous third-party databases.

Automated checks can be easily conducted against **databases of known stolen documents**, as well as fraudulent and synthetic identities.



A combination of static images and live video are captured either **remotely or in person**.

Physical features and information from official identity documents are used to perform an **advanced biometric comparison**.

Results are provided in real-time, **automatically taking into account risk factors** in relation to fraudulent identity, digital tampering and suspect lighting conditions.

Joint Statement in support of digital identity technology in the legal sector

- One often cited barrier to adopting digital ID tools is that to do so would put the user in breach of their obligation not to outsource their AML responsibilities. It is correct that a legal professional cannot outsource their *responsibility*, but this does not stop the use of digital ID tools in supporting CDD, which is permissible within the legal services regulatory frameworks of each jurisdiction of the UK. Legal practitioners will remain liable for their AML responsibilities, whether they use manual or digital methods of identity verification, and will need to ensure that verification is being carried out in line with the appropriate guidance.⁷
- The Joint Money Laundering Steering Group (JMLSG) Prevention of Money Laundering/Combating Terrorist Financing Guidance s2.17 says “Nothing in the ML Regulations prevents a firm applying CDD measures by means of an agent or an outsourcing service provider (but see paragraphs 5.3.51 to 5.3.53 in Part I, Chapter 5), provided that the arrangements between the firm and the agent or outsourcing service provider provide for the firm to remain liable for any failure to apply such measures.”

“Digital identity technology has come on leaps and bounds in recent years and if used properly can be a good way of mitigating the risks of money laundering, fraud and identity theft. Technology is an increasingly important tool in the fight against financial crime.”

Colette Best,
Director of AML, Solicitors Regulation Authority

“Without the use of new digital technologies such as for ID purposes, our drive to reduce the onboarding and exchange times for transactions would be severely held back. Given that we now rarely meet our clients, it’s never been more important for us to use robust and effective software solutions across the entire business.”

Peter Ambrose,
Managing Director The Partnership Limited

“Typically the first thing we’re asked by prospective clients across sectors is ‘How is your technology and approach viewed by our regulator’. This joint statement is testament to the collaborative and practical approach taken by key UK regulators, aligning with a standards based approach to the value, adoption and implementation of digital ID.”

Callum Murray,
Director of AML, Founder/CEO Amiqus

⁷ - Note that under the UK Government’s upcoming Digital Identity and Attributes Trust Framework, digital identity providers will be newly required to accept a degree of liability.

“Before using digital ID technology, waiting for certified copies of clients’ ID could take anywhere from two weeks to two months. It was frustrating for our clients and our legal teams. Now, we can complete client verification in as little as one working day. We have seen a big reduction in the number of files where ID causes issues or delays. It has made for a more frictionless experience for both client and lawyer, as well as improving our compliance procedures.”

Emma Gilroy,

Director & Head of Residential Property, JCP Solicitors

What’s next?

- In the UK, the Government is developing the UK Digital Identity and Attributes Trust Framework (UKDIATF), which seeks to make it easier and more secure for people to use services that enable them to prove who they are or something about themselves. Those using the trust framework will be able to describe attributes and digital identities they have created in a consistent way. Identity Service Providers that are certified against the trust framework will be trust-marked, allowing them to demonstrate to users that they meet government standards and are adhering to the rules.
- Sector-specific trust schemes are being developed under the framework, for example in the conveyancing sector, to reduce the burden on home buyers and sellers by allowing them to use one certified identity check as opposed to several over the course of the process.

- Wider schemes are also being developed globally, for example by the Digital Government Exchange (DGX), who released a set of principles to support the interoperability of digital identities between nations in the future.⁸
- Greater adoption and standardisation will be a key part of mitigating money laundering and the financing of criminality over the coming years. Digital ID verification is here now, and is increasingly being used in legal and other sectors. National frameworks will help ensure consistency between services and organisations, and allow users greater control over the data they provide.
- The legal services regulators support the ongoing development and adoption of responsible technologies, processes and standards around digital ID and client onboarding, that benefit clients and uphold trust in the legal sector.

Conclusions

- No regulator in UK jurisdictions prevents the use or reliance on digital means of identity verification in legal services. Responsible selection, adoption and implementation of these tools can contribute to improved compliance practices across the legal sector, as well as improved client service.
- Digital identity technology has become a valuable tool in combating money laundering risk across industries worldwide. It is critical the

⁸ - [Digital Identity in response to COVID-19](#)

Joint Statement in support of digital identity technology in the legal sector

legal community keeps up with advancements in technology and responsibly deploys them to the benefit of their clients and wider society.

- The Regulatory Response Unit (RRU) encourages all legal practitioners to review their client onboarding and AML practices in light of the available technologies and use the resources and support available to evaluate and responsibly deploy them.

Further Resources

For those seeking to adopt digital ID tools, there are a number of resources available to assist with understanding and compliance.⁹ You may wish to visit the following for more information:

- [DCMS Digital Identity and Attributes framework](#) - the proposed set of rules developed by DCMS, for organisations to follow if they want to provide secure and trustworthy digital identity and/or attribute solutions.
- [Legal Services Affinity Group \(LSAG\) AML Guidance](#) - s6.14.3 on Electronic verification provides detailed guidance from LSAG.
- [Government Good Practice Guide 45 - How to prove and verify someone's identity](#) - guidance from Government on the standards required to check and verify someone's identity.
- [HMLR Practice guide 81: encouraging the use of digital technology in identity verification](#) - details the use of the HMLR 'safe harbour' standard, for conveyancers using biometric and cryptographic technology for verification purposes.
- [Home Office - Identification Document Validation Technology](#) - comprehensive guidance from the Home

Office relating to the use of ID document validation technology.

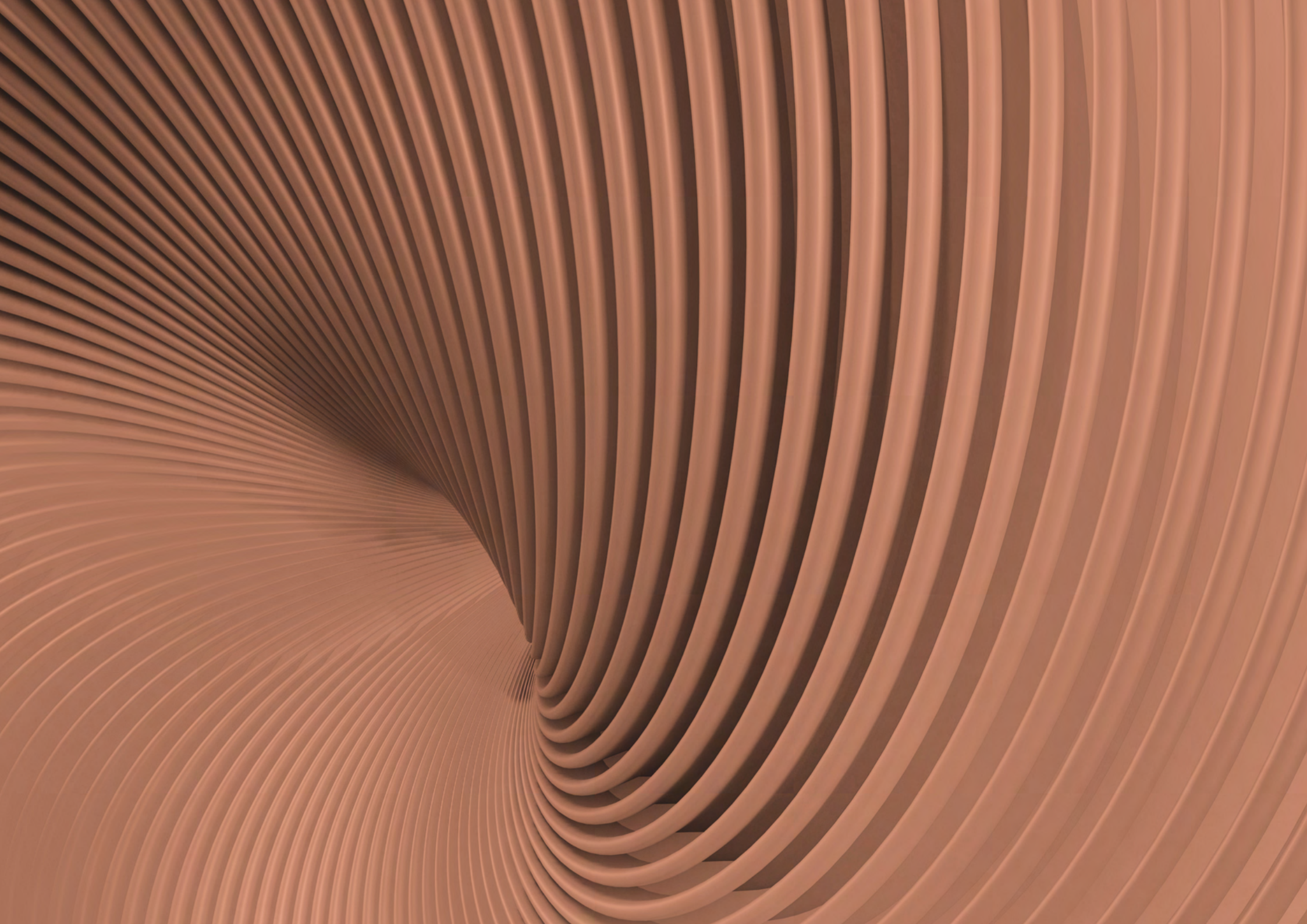
- [Financial Action Task Force \(FATF\) - Digital Identity](#) - guidance from an independent inter-governmental body on the use of digital identity technology in financial services.
- [Joint Money Laundering Steering Group \(JMLSG\) - Prevention of Money Laundering/ Combating Terrorist Financing](#) - sets out what is expected of firms in relation to the prevention of money laundering and terrorist financing.

⁹ - Please note that neither the RRU or LawtechUK are responsible for the upkeep of the listed resources. Any questions relating to them should be directed to the domain owner to which the resource belongs.

About the Regulatory Response Unit

The Regulatory Response Unit (RRU) brings relevant regulators together into a single, fast response forum, to make it easy for those innovating in the legal sector to access and navigate the rules and move forward with confidence.

The legal services regulators participating in the RRU have developed this guidance in consultation with digital ID tool providers seeking to make identity verification easier and lower risk for all concerned, including Amicus, Legl and Thirdfort.



LAWTECH 

TECH 
NATION