

Improving the effectiveness of the Money Laundering Regulations

techUK's response to the HMT consultation

June 2024

Contact: 10 St Bride Street, London, EC4A 4AD
Telephone: 020 7331 2000
Email: info@techUK.org

About techUK

[techUK](#) is a membership organisation launched in 2013 to champion the technology sector and prepare and empower the UK for what comes next, delivering a better future for people, society, the economy and the planet.¹

It is the UK's leading technology membership organisation, with more than 1,000 members across the UK, operating in areas including digital identity, national security and financial services. We are a network that enables our members to learn from each other and grow in a way which contributes to the country both socially and economically.

By working collaboratively with government and others, we provide expert guidance and insight for our members and stakeholders about how to prepare for the future, anticipate change and realise the positive potential of technology in a fast-moving world.

Background

On 11 March 2024 [HM Treasury published a consultation](#) on improving the effectiveness of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the 'MLRs'), which place requirements onto a range of businesses to identify and prevent money laundering and terrorist financing.²

The Ministerial Foreword from Baroness Vere states:

"The UK's Money Laundering Regulations (MLRs) form a vital bulwark against the proceeds of crime entering the UK financial system. With new technologies being developed and continuing global threat from economic crime and illicit finance, it is more important than ever that we give businesses the right tools to identify and prevent money laundering and terrorist financing. A balanced and effective AML/CTF (anti-money laundering and counter-terrorist financing) regime protects the UK's reputation as a modern, safe place to do business, and protects the integrity of the financial system. As a global issue, it is crucial that the UK

¹ techUK, the UK's technology trade association: <https://www.techuk.org/>

² "Improving the effectiveness of the Money Laundering Regulations" (HM Treasury, 2024). Available at: <https://www.gov.uk/government/consultations/improving-the-effectiveness-of-the-money-laundering-regulations>

continues to show leadership on economic crime, driving up standards worldwide and involving the private sector as an active partner.”

During the consultation period, HM Treasury (HMT) held a series of virtual, working-level events to discuss the consultation with interested stakeholders, and which techUK attended. This open letter to HM Treasury is techUK’s response to the consultation.

Digital ID

Money laundering is a significant issue in the UK, with an estimated £10bn laundered through the country each year.³ Traditional methods of identity verification, such as physical documents, are often time-consuming, prone to error, and can be easily exploited by criminals.

Digital ID technology is emerging as a powerful tool in the fight against money laundering in the UK. By providing a secure, efficient, and cost-effective means of identifying individuals, it can significantly enhance the effectiveness of AML measures. Digital ID technology offers a more robust solution by enabling financial institutions to carry out customer due diligence (CDD) and Know Your Customer (KYC) checks more accurately and efficiently. This can help to identify suspicious activities more quickly, reducing the risk of money laundering.

techUK are pleased that this consultation has a section dedicated to enhancing the role this technology can play to assist government, regulators and law enforcement in combating money laundering.

Strengthening understanding of Digital ID

The potential benefits of digital ID technology in combating money laundering are clear. For instance, the UK Financial Intelligence Unit receives around 460,000 Suspicious Activity Reports (SARs) a year.⁴ With the aid of digital ID technology, the processing of such reports could become more efficient and accurate.

³ “Biggest ever crackdown on money mules in the UK,” (Home Office, 2024). Available at: [https://www.gov.uk/government/news/biggest-ever-crackdown-on-money-mules-in-the-uk#:~:text=Cifas%20estimates%20that%20there%20were,National%20Crime%20Agency%20\(NCA\).](https://www.gov.uk/government/news/biggest-ever-crackdown-on-money-mules-in-the-uk#:~:text=Cifas%20estimates%20that%20there%20were,National%20Crime%20Agency%20(NCA).)

⁴ Suspicious Activity Reports (SARs), National Crime Agency (NCA). Available at: <https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/money-laundering-and-illicit-finance/suspicious-activity-reports>

Moreover, the Solicitors Regulation Authority submitted 24 suspicious activity reports relating to assets totalling more than £75m in the last year.⁵ The use of digital ID could streamline this process, making it easier to track and report suspicious activities.

Our observation from attending stakeholder calls hosted by HMT as part of this consultation process is that within the AML community (including banks, insurers, property agents, auditors, auction houses), there was a deficiency in knowledge as to what Digital ID is and the benefits it brings – potentially hampering the positive impact it can have.

techUK as the UK's trade association for technology has a [significant number of Digital ID firms within membership](#)⁶, and so we believe we are ideally placed to facilitate broader engagement to build knowledge and confidence in these technologies. We offer HMT an open door to explore how we can work with them to assist this capacity-building across the ecosystem.

Call to Action:

HMT should work with techUK to help build awareness and confidence in utilising Digital ID to help in efforts against money laundering.

Digital ID and implementation of the Trust Framework

The Department for Science, Innovation and Technology (DSIT) has created a “digital identity and attributes governance framework” (also known as the “Trust Framework”) which governs private sector suppliers of digital verification services. This framework set out the rules for the future use of digital identities. It aims to create a process as trusted as using passports or bank statements, thereby enhancing the reliability of identity verification.⁷ The Trust Framework also recognised the plurality of roles and business models in the UK digital ID ecosystem.

The implementation of the Trust Framework could significantly aid anti-money laundering efforts. However, its effectiveness will depend on the robustness of the Trust Framework and the extent to which it is adopted by relevant institutions.

⁵ Anti-Money Laundering annual report 2022-23 (Solicitors Regulation Authority, 2023). Available at: <https://www.sra.org.uk/sra/research-publications/aml-annual-report-2022-23/>

⁶ techUK's Digital ID programme: <https://www.techuk.org/accelerating-innovation/digital-identity.html>

⁷ “Impact assessment: Data Protection and Digital Information (No. 2) Bill: European Convention on Human Rights Memorandum,” (DSIT and DWP, 2023). Available at: <https://www.gov.uk/government/publications/data-protection-and-digital-information-bill-impact-assessments/data-protection-and-digital-information-no-2-bill-european-convention-on-human-rights-memorandum#summary-of-the-bill>

Because of this, it's imperative that MLRs make reference to the Digital ID providers who adhere to the DSIT Trust Framework. This not only ensures that good governance is in place in accordance with the framework, but it gives business and consumers the confidence that utilising these technologies are in accordance with relevant regulatory requirements – something which is crucial for adoption by financial institutions.

Call to action:

HMT should make reference in its MLRs to the Trust Framework for digital ID.

Digital ID and robustness of the Trust Framework

The recent Data Protection and Digital Information Bill (No. 2)⁸ included provisions to enshrine this Trust Framework in law: unfortunately, despite these clauses being uncontentious, on 30 May 2024 (during this HMT consultation period) the Bill fell at the final Report stage when Parliament was dissolved for a General Election.

The Trust Framework is needed in statute to ensure robustness of governance and standards, and also to underpin trust from financial institutions, businesses and customers.

Call to action:

HMT should work with DSIT to ensure that the Trust Framework is enshrined in law urgently.

Digital ID and effectiveness of the Trust Framework

The Trust Framework governs industry, but it's not yet clear to techUK members how the public sector will align with it for harmonisation and interoperability. This ambiguity risks undermining the broader digital ID ecosystem in the UK, as well as public and consumer confidence in the technology. Ambiguity and lack of interoperability would be harmful to HMT's efforts to combat money laundering.

⁸ Data Protection and Digital Information (No. 2) Bill, UK Parliament (24 April 2024). Available at: <https://bills.parliament.uk/publications/55222/documents/4745>

Call to action:

HMT should work with DSIT to ensure that the Trust Framework governs the public sector as well as industry, for robust, effective and frictionless AML activities.

Digital Assets

Digital assets aim to provide disruption to traditional models in finance and payments, driving changes in the broader financial ecosystem. Examples of digital assets include cryptocurrencies and tokenisation.

Digital assets have experienced rapid growth, with 516m cryptocurrency users worldwide⁹ and a daily trading volume of \$116.61bn per 24 hours.¹⁰ The global market capitalization of cryptocurrencies was approximately \$2.37tn on 31 May 2024.¹¹

Advocates of cryptocurrency argue they bring benefits such as decentralisation, which means cryptocurrencies aren't controlled by institutions or governments; security, because it is difficult to counterfeit transactions; privacy, because cryptocurrencies enable payments without disclosing personal information; global accessibility, because of enabling anyone with an internet connection to use cryptocurrency; and speed or efficiency, compared to traditional banking and money transfer systems.

However, many of these benefits of cryptocurrencies also pose challenges to governments, regulators and financial institutions because of the anonymous nature and ease in setting up a wallet¹². The UK has been proactive in addressing the challenges posed by digital assets, such as cryptocurrencies, particularly in relation to money laundering. The Financial Conduct Authority (FCA), the country's financial regulator, has been at the forefront of these efforts.¹³

⁹ "Blockchain Statistics of 2024" (DemandSage, 2024). Available at: <https://www.demandsage.com/blockchain-statistics/>

¹⁰ "10 Cryptocurrency Statistics, Facts, and Trends in 2024," (Finrax Resources, 2024). Available at: <https://blog.finrax.com/10-cryptocurrency-statistics-facts-and-trends-in-2024>

¹¹ "Cryptocurrency Prices Today By Market Cap" (Forbes, daily tracker). Available at: <https://www.forbes.com/digital-assets/crypto-prices/?sh=6ea2e3562478>

¹² "Money laundering through cryptocurrencies" (UN Office on Drugs and Crime). Available at: <https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/laundryingproceeds/moneylaundering.html>

¹³ "Regulation of Digital Assets in the UK," (Speech by Sarah Pritchard, Executive Director of Markets and Executive Director of International, FCA 2023). Available at: <https://www.fca.org.uk/news/speeches/regulation-digital-assets-uk>

Proportionality

techUK members have expressed a desire that the MLRs are implemented proportionately, in that care is exercised to ensure they only are introduced where they add value.

It is also notable that in 2023, the value received by identified cryptocurrency addresses fell significantly from \$39.6bn to \$24.2bn.¹⁴ This could be due to technology providers, several of whom are in techUK membership, improving the ability for institutions to identify wallets associated with criminal or terrorist activity and blocking payments from taking place; and the impact of crypto regulatory regimes being implemented. This indicates that an overhaul of the MLRs may not be needed, and/or that any updates to the MLRs should be cognisant of the evidence of the impact of new technology solutions operating under existing regulations.

Call to action:

HMT should deliver a proportionate approach to the revision of MLRs, introducing new requirements only where they will add value and deliver against the desired outcomes.

Information-sharing

techUK members recognise that almost every sector can leverage crypto assets, and so believe there is a further role for delivering cross-sector insights in money laundering in order to fully appreciate where it may be evolving. This is an area where MLRs could play a role in facilitating those information flows to help strengthen intelligence and better identify trends and risks.

Call to action:

HMT should consider how MLRs can help to facilitate greater sharing of information from all sectors where digital assets can be leveraged, to provide a much fuller picture of trends and intelligence.

¹⁴ “2024 Crypto Crime Trends,” (Chainalysis, 2024). Available at: <https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/>

National Risk Assessments

A challenge for both government and regulators is that National Risk Assessments (NRAs) are only snapshots in time, and therefore can become outdated very quickly.

techUK members include companies that are able to conduct real-time risk analysis, and so there may be an opportunity to collaborate on how the public and private sectors can work together to develop products and solutions to respond to this challenge.

Call to Action:

HMT and regulators should work with industry to better understand solutions that can help deliver real-time analysis of risk beyond National Risk Assessments.