WHITEPAPER

The future of digital compliance: Predicting trends and preparing for tomorrow's challenges

SmartSearch®

SmartSearch
Mayfield House, Lower Railway Road, Ilkley, LS29 8FL

smartsearch.com

Why compliance should be a key priority in 2025

As 2024 comes to an end, it is a great opportunity for regulated firms to reflect on the compliance challenges they have faced this year and prepare for the road ahead.

This year has seen significant shifts in regulatory requirements, advancements in technology – especially AI - as well as increasing complexity in areas like data privacy, and cybersecurity.

By reviewing the last year, regulated firms can address any compliance problems they encountered in the past 12 months, and get a head start on any potential new challenges to ensure they are in a strong position as they go into 2025.

So to help, in this Whitepaper, we look at how continuous advances in AI technology, the ever-complicated issue of balancing customer compliance with data privacy, the continued growth of cryptocurrencies and other digital payment channels, and an ever-changing regulatory landscape will shape the AML trends to watch out for in 2025. And more importantly, how firms can look to tackle these compliance challenges in the most cost-effective way.

Advances in AI - the challenges and opportunities

Huge advances have been made in the field of AI and machine learning over the past year. And while the ability to simulate human behaviour - in text, video and audio – is seen as a positive development by many, the potential for misuse of this type of technology is considerable, especially when it comes to ‘deep fakes’.

Deep fakes – which is where fraudsters use AI-generated video or audio to replicate someone's voice, image, and movements – are becoming increasingly hard to distinguish from the real thing. For example, earlier this year, an employee of a multinational company thought he was logging into a virtual meeting with his organisation's CFO and co-workers. Initially sceptical, he dismissed concerns after joining the call, where the participants appeared familiar. However, none of the others on the call were real—they were AI-generated deep fake recreations. During the call, the fake CFO instructed him to transfer $25 million to multiple Hong Kong bank accounts controlled by criminals. It wasn't until later that he realised he had been scammed.

While in the UK, fraudsters created a deep fake of Martin Lewis – the trusted consumer champion, and Elon Musk, who is well known for his support of crypto currency - to defraud victims out of thousands in a bitcoin scam.

This manipulation of AI is only going to get more sophisticated, and as a result, 2025 could also be one of the most challenging for regulated firms as they race to build crime fighting solutions as fast as AI is developing.

And that is where AI - and other advanced compliance tools - can be used for good. For example, using AI in combination with database identity verification is the best way to fight AI-enabled fraud. This is because AI is able to process vast datasets accurately and efficiently and deliver rapid results, which not only enhances the user experience but also strengthens trust in the data. For example, even if a fraudster managed to create a deep fake that is able to bypass ID checks, they cannot insert fake records into all the relevant sources - electoral registry, credit system etc - so it would be flagged.

Striking the balance between transparency and privacy

One of the biggest challenges within AML and anti-corruption, is how to balance AML with responsible personal data use. On the one hand, regulated firms need access to personal and financial data in order to ascertain risk and potential for wrongdoing. On the other, being able to access this level of data is seen as a breach of privacy – and potentially, ironically, could leave individuals vulnerable to fraudsters.

And in fact, the EU recently passed a law that found that the EU Anti Money Laundering Directive that there must be a central Ultimate Beneficial Owner register 'violates fundamental EU privacy and personal data protection rights'.

However, transparency and privacy are not contradictory; using personal information to combat financial crime while respecting privacy is both possible and essential, and will be one of the key compliance challenges in 2025.

In the UK, we have laws in place to protect privacy – like GDPR - which many see as a hindrance to AML effort. This is because GDPR requires companies to obtain explicit consent from users before collecting their personal data and provide them with the right to access, correct, and delete their data. Companies that fail to comply with these regulations face severe penalties, including fines of up to 4% of their global revenue. This, understandably puts companies off from collecting data, which means many are failing to check customers properly and putting themselves at risk.

What we need is a balance – and better understanding – of the rules. For example, the UK's Data Protection Act explicitly allows data sharing for anti-money laundering purposes. Therefore, a key focus going into the new year will need to be ending financial secrecy while retaining privacy. Key to this will be public access to company ownership information, better collaboration between regulators, firms and users, high level privacy policies in place and the strategic use of advanced technology within verification, data hosting and data analytics. Third-party verification, screening and data hosting tools will be a key part of the solution for regulated firms.

The rise and rise of crypto

Bitcoin is just a few thousand dollars away from hitting $100,000 after a sharp rise following Donald Trump's re-election victory, and analysts believe that the world's leading crypto currency will continue its upward trajectory into 2025 under his pro-crypto presidency.

His second term is likely to further legitimatise the industry and even establish bitcoin as a ‘mainstream’ asset, that can hedge inflation. And while crypto’s position as a potential ‘safe-haven’ for investors during tumultuous times is debatable, what is not under question is its vulnerability in terms of financial crime.

Thanks to its accessibility, anonymity and strong allegiance with social media platforms – the crypto market is already one of the most targeted sectors when it comes to money laundering and financial crime; according to the Federal Trade Commission, scammers collected $679 million in cryptocurrency in the first half of 2024, making it the most lucrative payment method behind only bank transfers.

And as it continues to rise both in value and popularity – according to the FCA, 12% of UK adults now own crypto, up from 10% - it will become an even more significant compliance challenge going into 2025.

Crypto remains a relatively unregulated market, so the key to fraud prevention will be to go above and beyond current legislation. Firms need to ensure that they have tough anti-money laundering an anti-fraud checks in place, including stringent verification procedures, robust financial checks, water-tight data hosting and real-time monitoring.

Stricter regulation and tougher penalties for non-compliance

According to the National Crime Agency fraud is now the most commonly experienced crime in the UK. It accounts for more than 40% of all crimes, with an estimated 3.5 million incidents recorded last year.

As a result, regulators are continually tightening the rules and increasing the penalties for non-compliance, with things set to become significantly tougher in 2025 with the introduction of the "failure to prevent fraud" offence.

Effective from 1 September 2025, this new legislation extends corporate liability for fraud committed by employees, agents, subsidiaries and 'associated persons' if the fraud benefits the organisation and has a UK connection. The key change here is that liability arises if the organisation lacks reasonable fraud prevention measures, regardless of where the entity is based.

As a result, we are likely to see organisations being forced to implement stronger internal controls, employee training, and monitoring systems, put in more checks when it comes to third-party relationships and be more proactive in terms of conducting much more regular compliance checks, with an emphasis on mitigation.

Regulators are likely to have more power in terms of pursing cases, while failure to comply could result in criminal prosecution as well as significant financial and reputational damage, it is therefore likely that this legislation will drive significant cultural and procedural changes and push those firms that are still failing to meet their compliance obligations to buck up their ideas.

We are also likely to see much stricter rules around crypto with Matthew Long, director of payments and digital assets at the FCA, saying that there is a "need for clear regulation that supports a safe, competitive, and sustainable crypto sector in the UK."

The solution

In the UK, all regulated businesses have a huge range of challenges to contend with as they enter 2025. These include the ongoing challenge of adapting office spaces to hybrid working trends, managing cultural and generation shifts – particularly in law firms where older partners' resistance to change extends beyond technology to overall work practices – as well as increasing client expectations and pressure to increase profits.

However, mitigating the risk of fraud while meeting compliance and data privacy obligations does not have to be one of them.

Third-party digital compliance platforms leveraging AI, behavioural analytics, biometric technology, and database identity verification offer a comprehensive solution to the increasingly complex compliance challenges firms face.

These platforms streamline customer onboarding and due diligence by efficiently processing vast datasets, enhancing the accuracy and speed of identity verification while reducing human error.

For example, AI-powered tools can detect fraudulent activities, such as deepfakes or synthetic identities, that might bypass traditional checks. Plus, their use ensures compliance with stringent regulations like GDPR while maintaining robust data privacy standards.

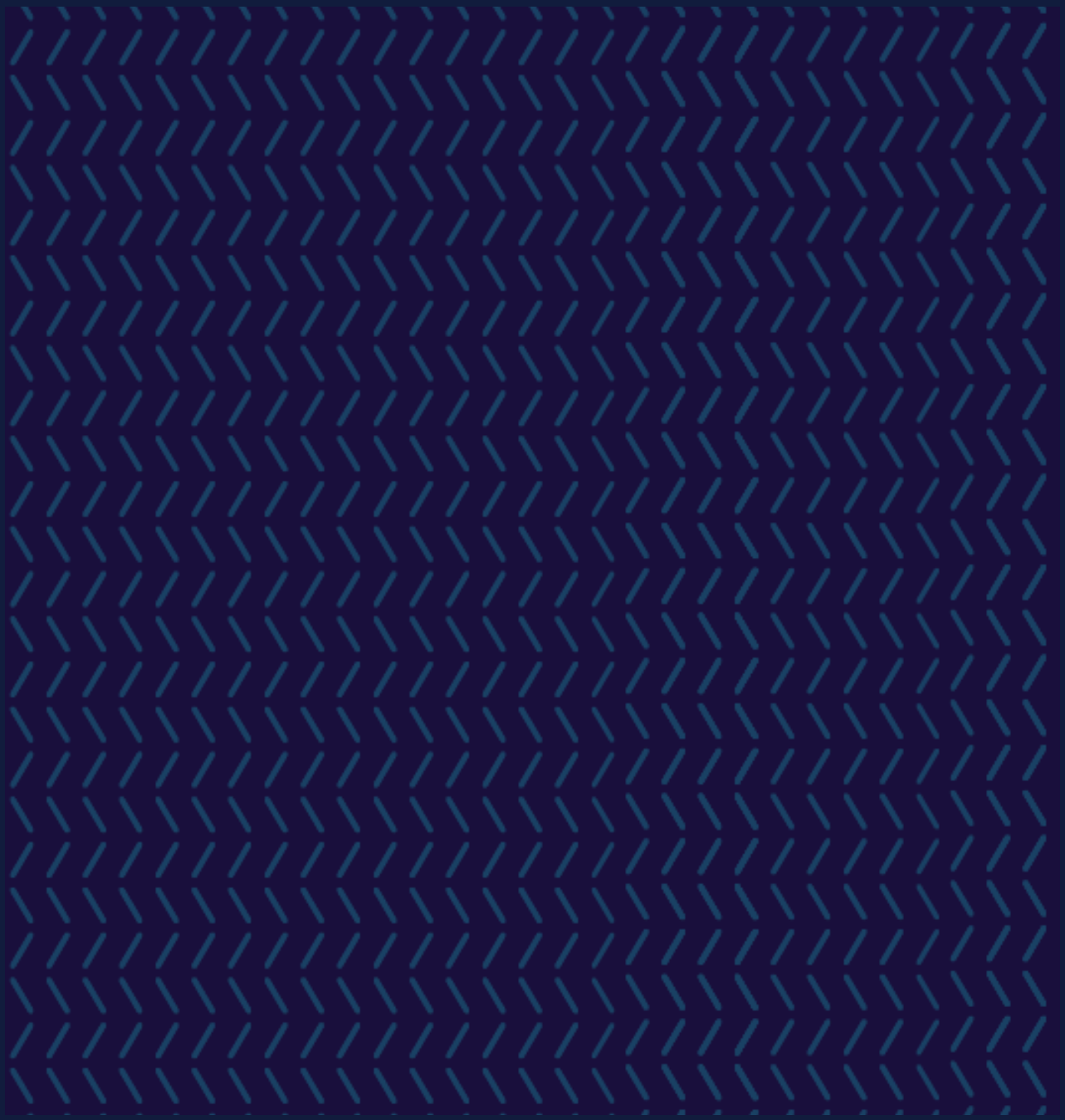
By integrating these technologies, firms can address challenges in areas like AML, cryptocurrency fraud, and the "failure to prevent fraud" offence, ensuring proactive risk mitigation and regulatory alignment in an evolving digital landscape.

About SmartSearch

SmartSearch is a market-leading all-in-one Anti-Money Laundering (AML), Fraud Prevention and Know Your Customer (KYC) platform which delivers award-winning AML verification for individuals and businesses in the UK and international markets.

SmartSearch's very latest technology delivers an unrivalled user experience to over 7,000 client firms and 60,000 users, enabling them to comply with the latest AML regulations.

For additional information on SmartSearch's services, or a free platform demonstration, please contact us on **info@smartsearch.com** or **01138688529**.



SmartSearch///

SmartSearch
Mayfield House, Lower Railway Road, Ilkley, LS29 8FL

smartsearch.com