fime × consult hyperion
consulting by fime

eBook

Bank identity verification

the challenge of supplier selection

Navigating compliance, functionality, quality, efficiency, security and more to future-proof customer onboarding and ongoing lifecycle management.

October 2025

consult hyperion

Contents

1. The changing fraud landscape.

Fraud is becoming increasingly sophisticated.

The rise in Artificial Intelligence (AI) has completely transformed the threat landscape, giving bad actors powerful tools to exploit both system weaknesses and human behaviors.

2025 is the first year where digital techniques have usurped physical counterfeiting.

The Entrust 2025 Identity Fraud Report states that digital forgeries have increased 244% in the last year, with deepfakes now accounting for 40% of all biometric fraud[1].

1 https://www.entrust.com/resources/reports/identity-fraud-report

This has been made possible by generative AI tools that can create convincing phishing emails and realistic identity documents in a matter of seconds.

These techniques, and more, are being used to impersonate trusted users during identity verification checks and fool biometric authentication systems.

Furthermore, these weapons are now being sold on in “fraud-as-a-service” models, enabling amateurs and lone actors to leverage sophisticated techniques that would historically only be available to high-budget operations.

2024 saw deepfake attempts occurred at a rate of one every five minutes. With bad actors growing in both confidence and in number, this figure seems to be set to become even more stark.

With regulations increasingly mandating strong identity verification during customer onboarding and lifecycle management and the ecosystem awash with different solutions, it can be complex, time consuming and potentially costly for banks to select and implement the right solutions to support their objectives.

2. The challenge for financial institutions.

back to contents

Critically, these fraudulent activities target both the Know Your Customer (KYC) activities at the initial onboarding phase and the ongoing authentication of customers and their accounts.

In this increasingly hostile digital environment, financial institutions are working to urgently address a few critical objectives:

- **Achieve and maintain regulatory compliance.**
- **Avoid financial loss due to fraudulent activities.**
- **Protect brand and retain customer trust.**

Achieve and maintain regulatory compliance.

This includes demonstrating adherence to stringent regulations within required timeframes. Many current and forthcoming regulatory updates now specify requirements around KYC, Anti-Money Laundering (AML), Customer Due Diligence (CDD) and more. Non-compliance can lead to hefty fines, reputational damage, and operational restrictions.

Avoid financial loss due to fraudulent activities.

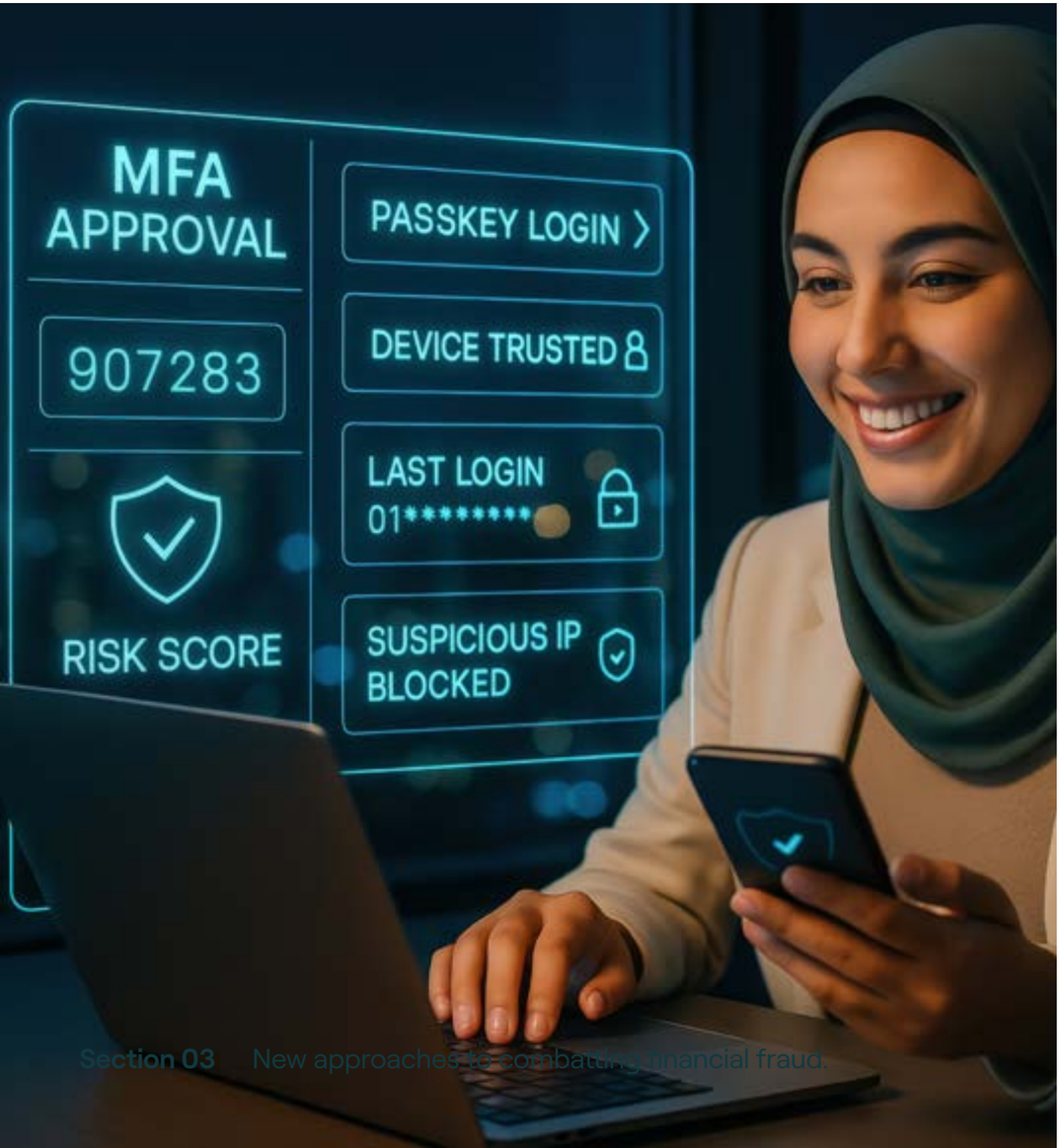
Direct financial losses from fraud can be substantial, impacting profitability and stability. Robust identity verification and fraud prevention mechanisms are essential to safeguard assets.

Protect brand and retain customer trust.

The proliferation of sophisticated attacks and fraud, such as account-take-over (ATO), deepfakes, and AI-powered scams, directly erode customer confidence and tarnish a bank's reputation. Maintaining trust is paramount in the competitive financial landscape.

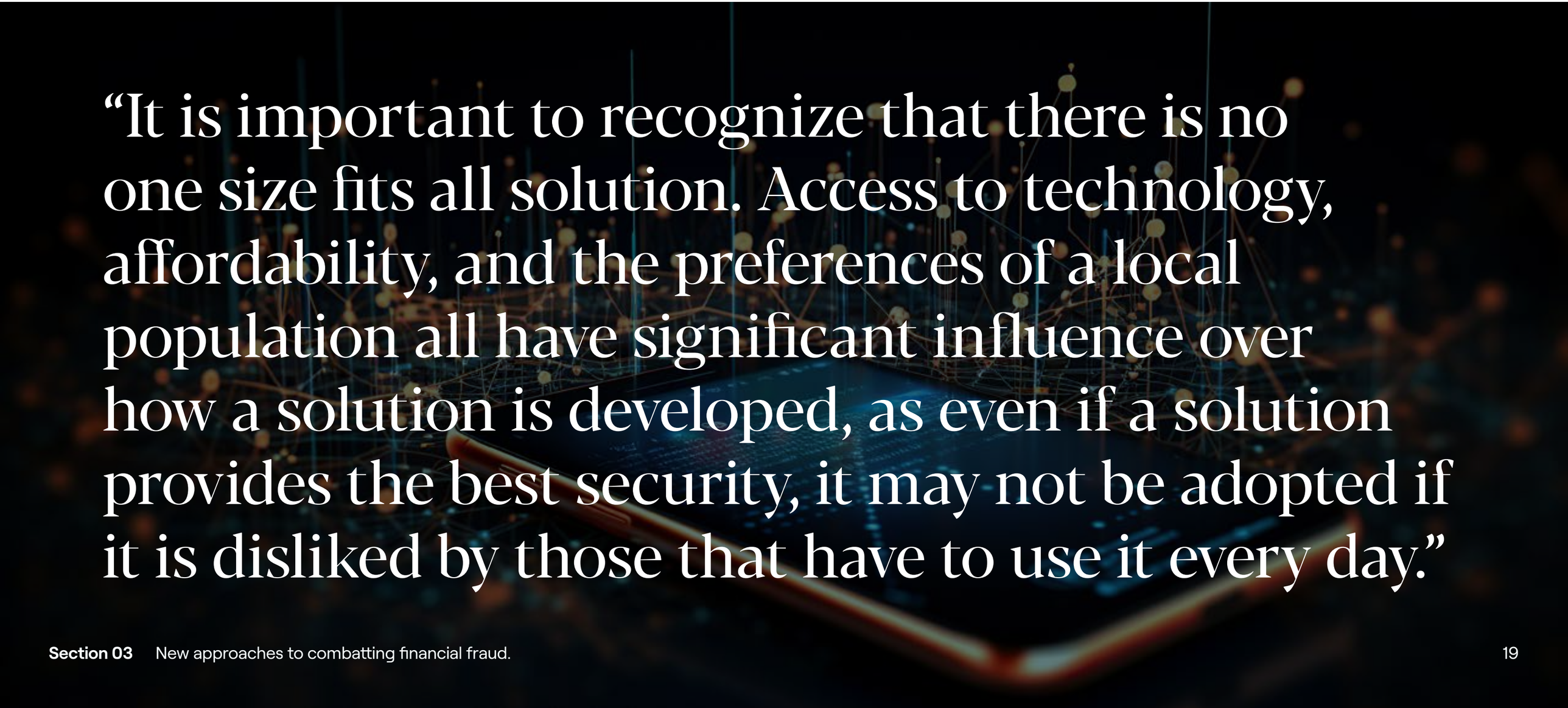
3. New approaches to combatting financial fraud.

In financial services, cybersecurity breaches and fraud can have catastrophic consequences, especially if the failure leads to the loss of a customer's money or their personal data.



Biometric authentication is therefore becoming increasingly mandated by central banks around the world, utilizing mainly fingerprint or facial recognition technologies to verify users. At the same time, behavioral biometrics are enhancing confidence that the ‘known’ user is using the application, without creating additional friction. This supports stronger multi-factor authentication (MFA) as it gives users a way to validate something they *are* in concert with the other pillars of MFA; something they have (such as a payment card), and something they know (a PIN or passcode).

Central banks and regulators are also accelerating their efforts to strengthen digital security, enhance identity verification, and combat financial fraud through several tactics and systems. KYC and AML regulations are non-negotiable, but it is vital that these provisions continue to evolve in response to the new threats posed by AI.



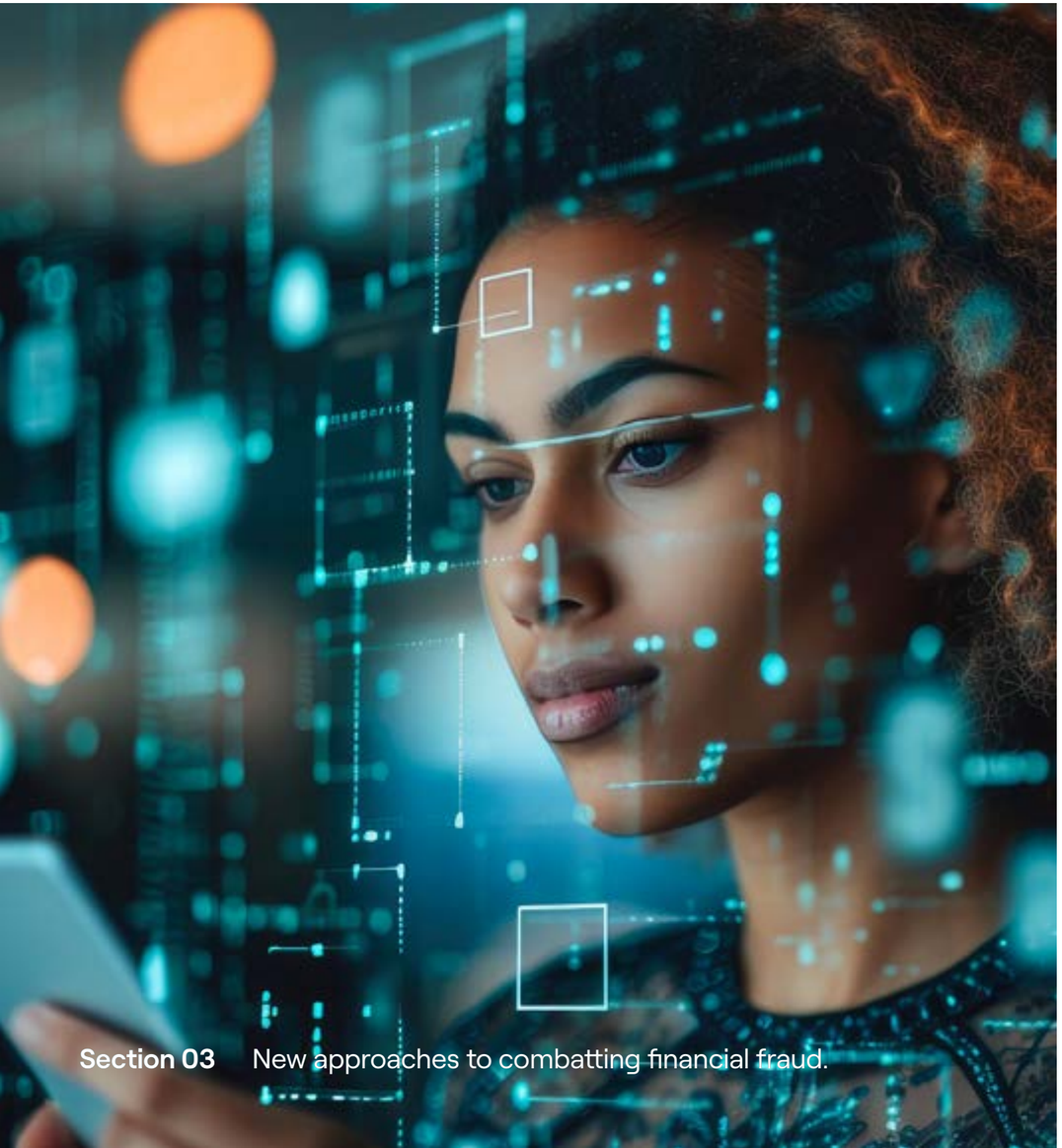
"It is important to recognize that there is no one size fits all solution. Access to technology, affordability, and the preferences of a local population all have significant influence over how a solution is developed, as even if a solution provides the best security, it may not be adopted if it is disliked by those that have to use it every day."

Several regions and nations are leading the way in creating a secure digital identity ecosystem:

In the **European Union**, the eIDAS 2.0 legislation established a continent-wide framework for seamless, trusted digital identity and authentication, meaning that provided a solution meets specified regulatory criteria, eIDs would be mutually recognized by all member nations and accepted by specified institutions.

The United States has seen significant progress in the deployment of mobile driver's license (mDL) solutions thanks to AAMVA's mDL Digital Trust Service (DTS), which provides a safe, secure and resilient means for relying parties to obtain verified public keys of issuing authorities.

Australia has introduced the Digital ID Act 2024, designed to provide a secure way for users to verify their identity for online transactions with both government and businesses. It supports this by formally establishing the dedicated Digital ID Regulator, enhancing governance and oversight.



These developments highlight a broader global trend in which countries are leveraging digital identity systems to strengthen the ability of banks to perform remote identity verification.

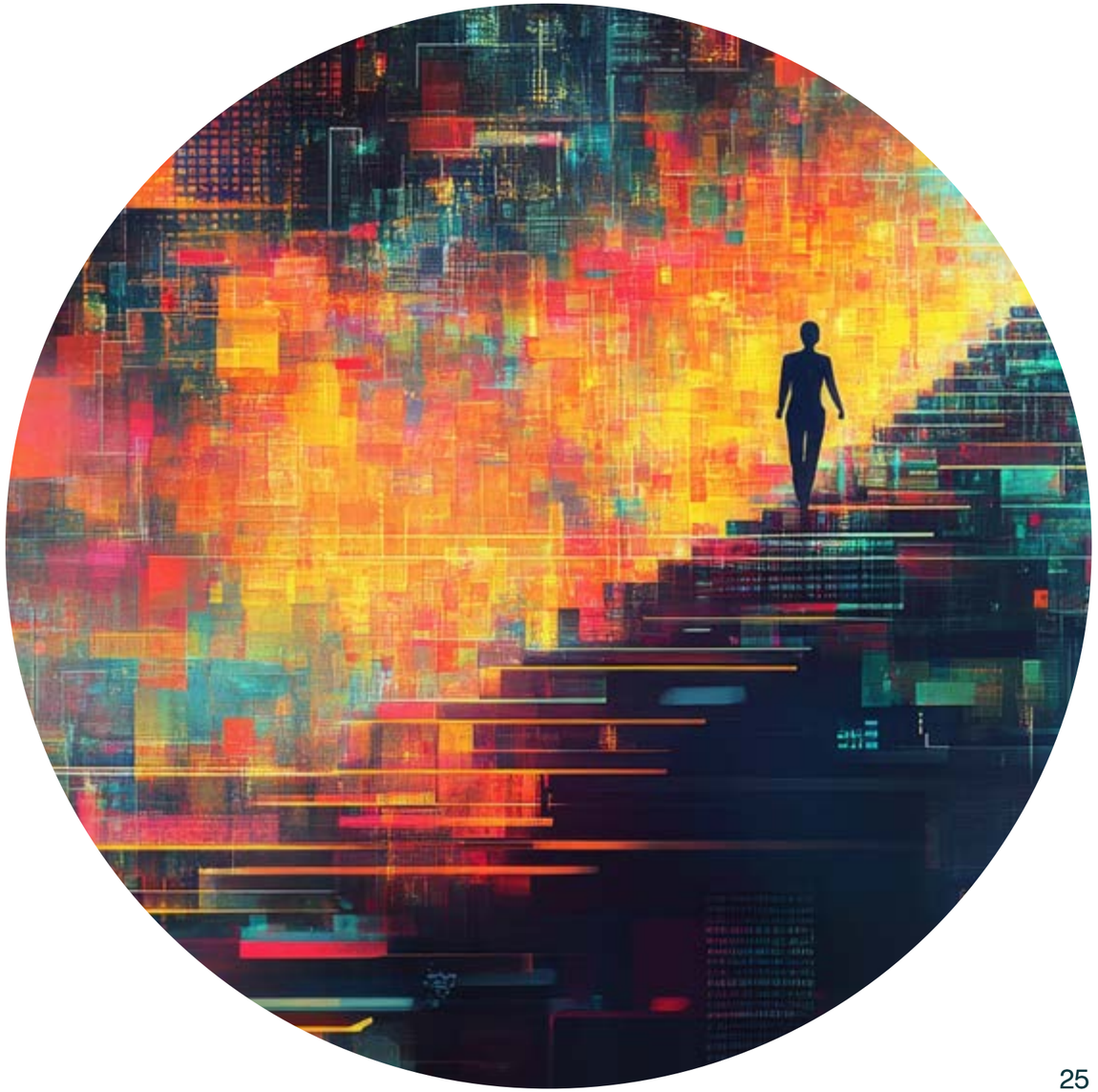
While the eID ecosystem and regulations are developing, banks and financial service providers need to rely on experts across domains to determine how these solutions can be integrated to support customer identification, authentication and mitigate fraud.

4. Robust identity verification processes.

To effectively combat fraud and meet regulatory demands, financial institutions must implement comprehensive identity verification solutions that address the entire customer lifecycle.

This lifecycle refers to the full journey from the creation of a customer identity during onboarding, through account management with ongoing activity monitoring and account recovery, to deactivation.

At each stage of the lifecycle, different identity verification requirements can be applied depending on the level of assurance required for risk assessment. For instance, liveness verification may be an important requirement to onboarding customers but may not be required for dormant account reactivation.



Regardless of the level of security required, the two fundamental processes that verification protocols should be based around are:

Identification – The process of establishing who the customer is.

This involves the customer providing evidence of their identity. Solutions leveraging biometrics for onboarding, combined with ID document verification and biometric matching, with liveness detection, are crucial. Support for remote onboarding processes and flexibility to adopt digital identity systems being built in the country are also vital considerations.

Authentication – Confirming that it is an authorized person making a transaction.

This process ensures that it is the legitimate user making the transaction under their own intention, not forced or performed by fraudsters. In this phase, different authentication methods can be used depending on the risk level of the transactions. Methods like biometrics can be used as a “step up” mechanism in cases where stronger authentication is needed, such as high value payments.

back to contents

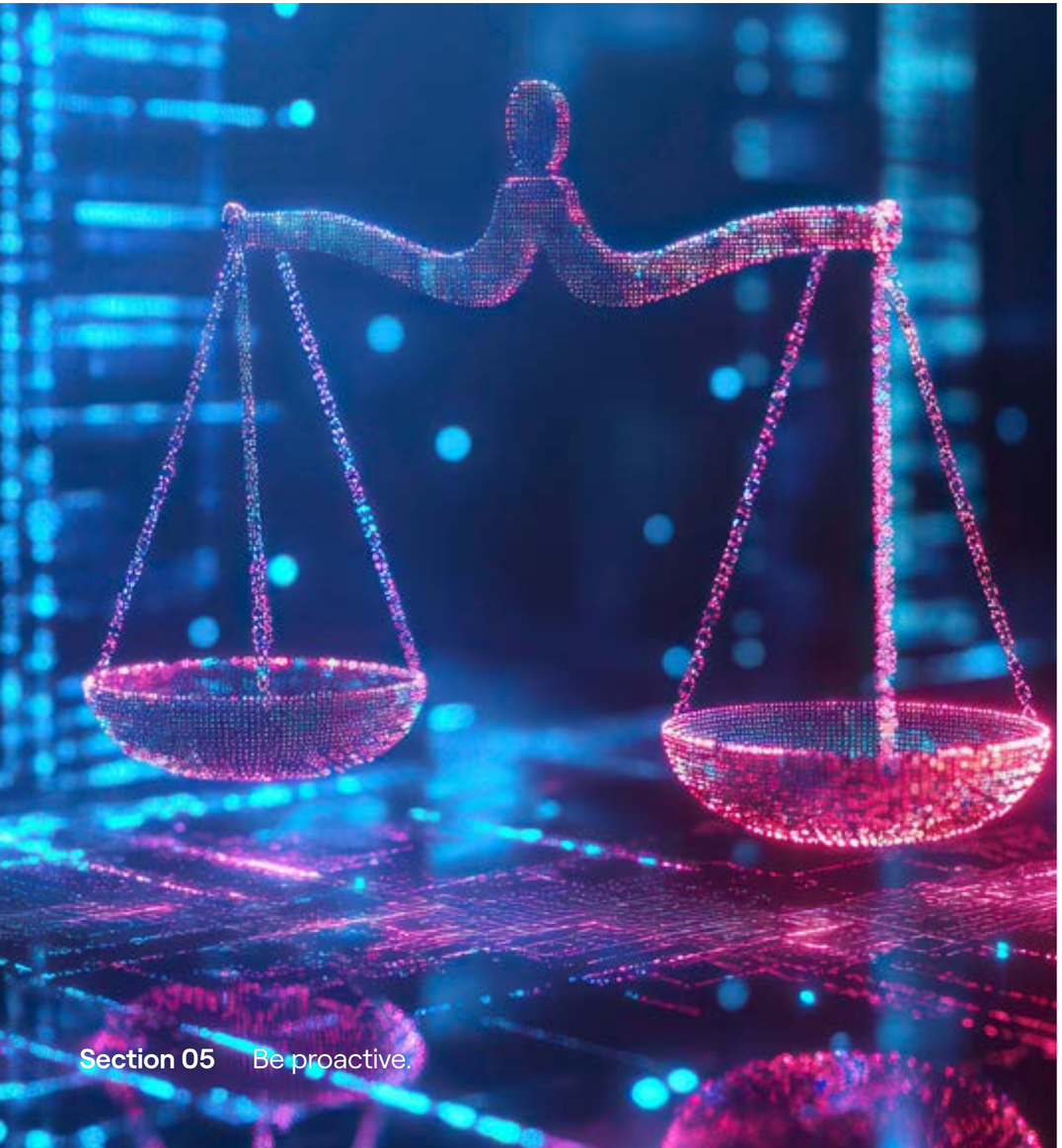
5. Be proactive. Not reactive.

With an ever-increasing number of threat vectors, and an evolving regulatory landscape, it is imperative that banks and financial service providers are proactive, not reactive, when developing their fortified digital identification and authentication infrastructure.

As explored in the previous section, there has been a strong emphasis on biometrics and multi-factor authentication. They now sit as foundational elements of several digital security offers, but they are not the only priorities.

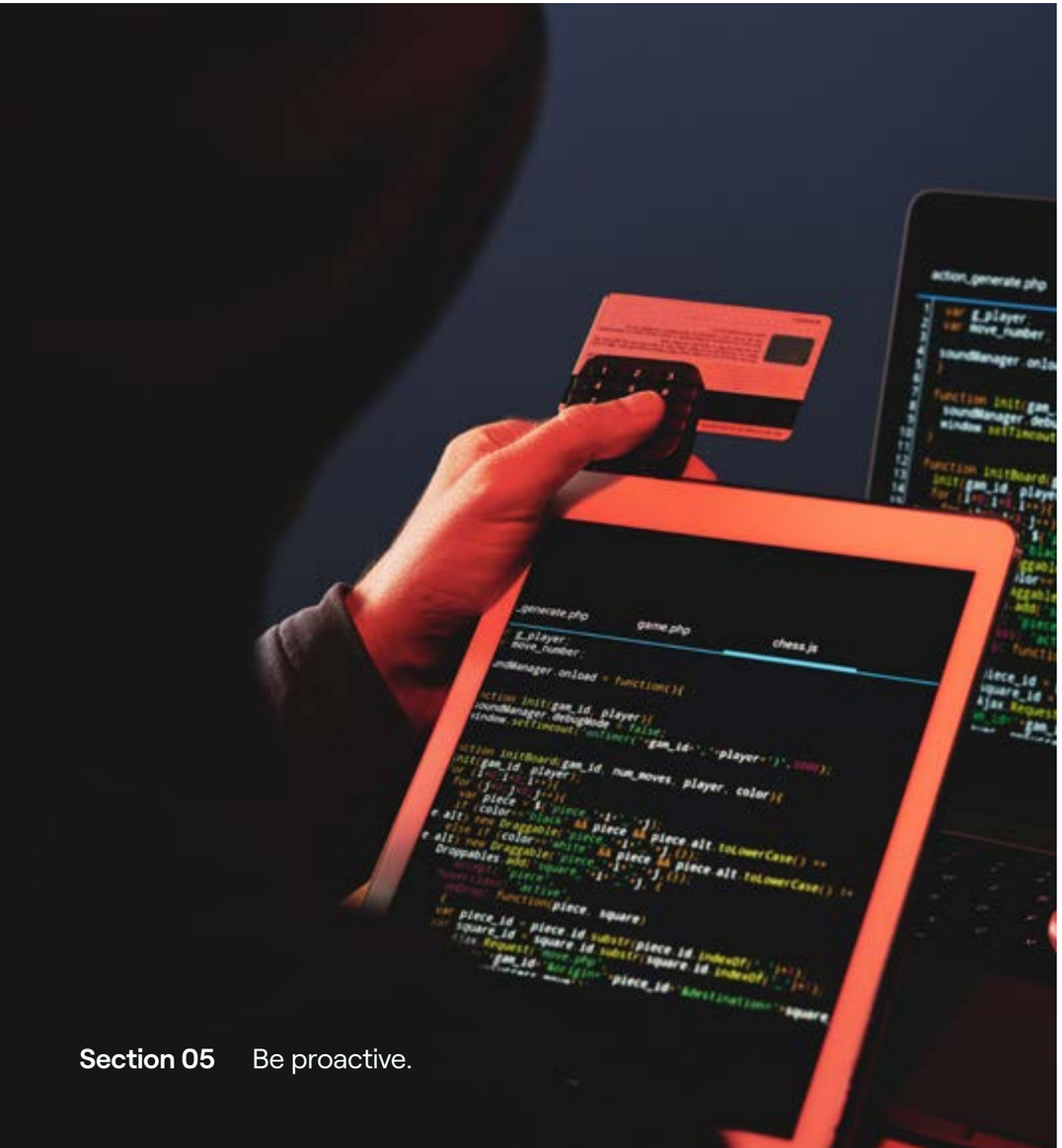
Those in charge of service digitalization and compliance departments at financial institutions are taking significant strides to upgrade their digital customer journey. Tactics include:

- **Find a balance between customer experience and security.**
- **Combating Sophisticated Fraud.**
- **Adopting International Standards.**
- **Due Diligence on Technology and Providers.**



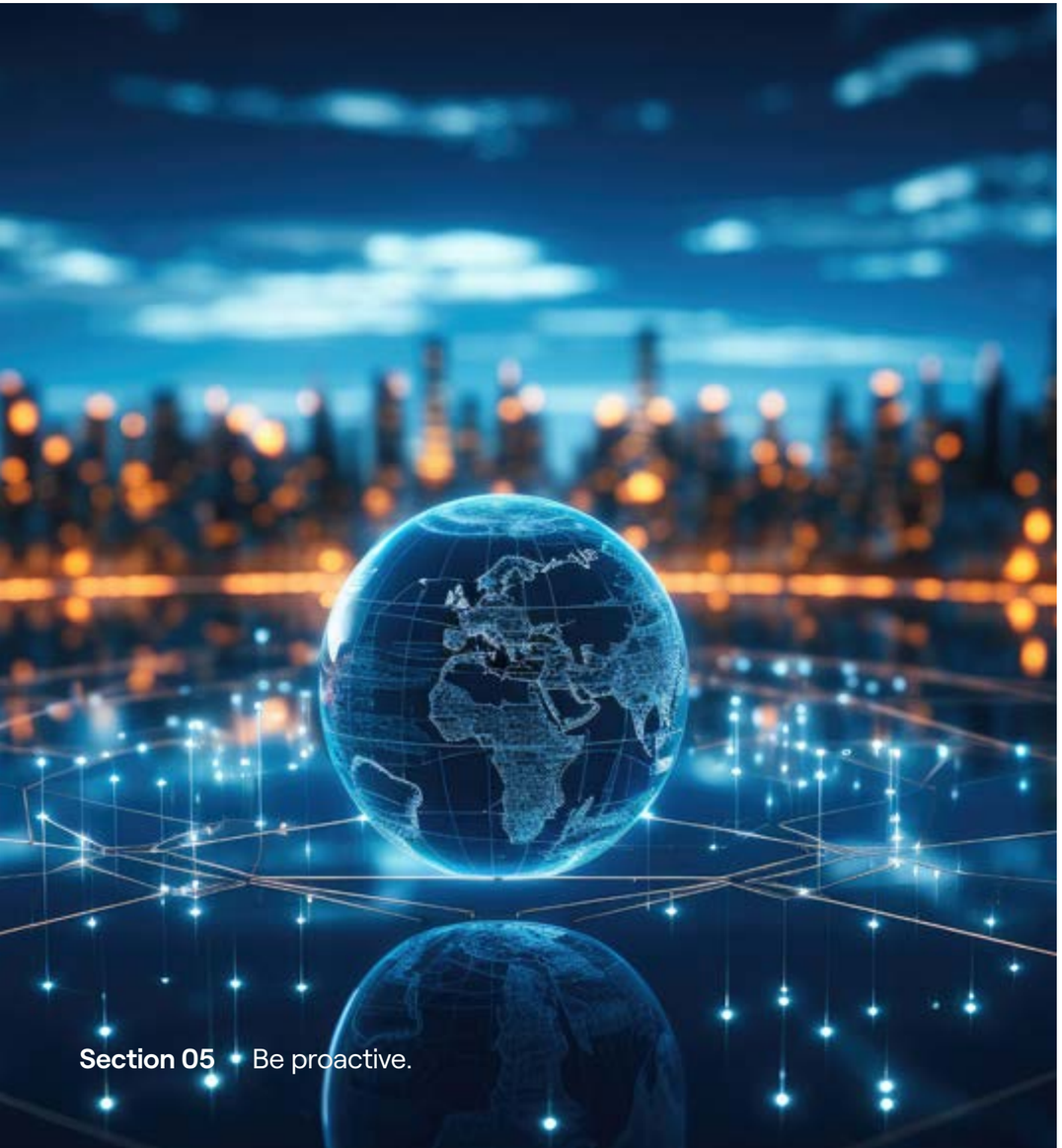
Find a balance between customer experience and security.

Different departments have different performance indicators to reach their goal, whether it is security, increasing customer onboarding, and/or growing transactions of existing customers. While evaluating how to enhance security and introduce innovations, it’s crucial to collaborate across departments to find a balanced approach across different strategic objectives.



Combating sophisticated fraud.

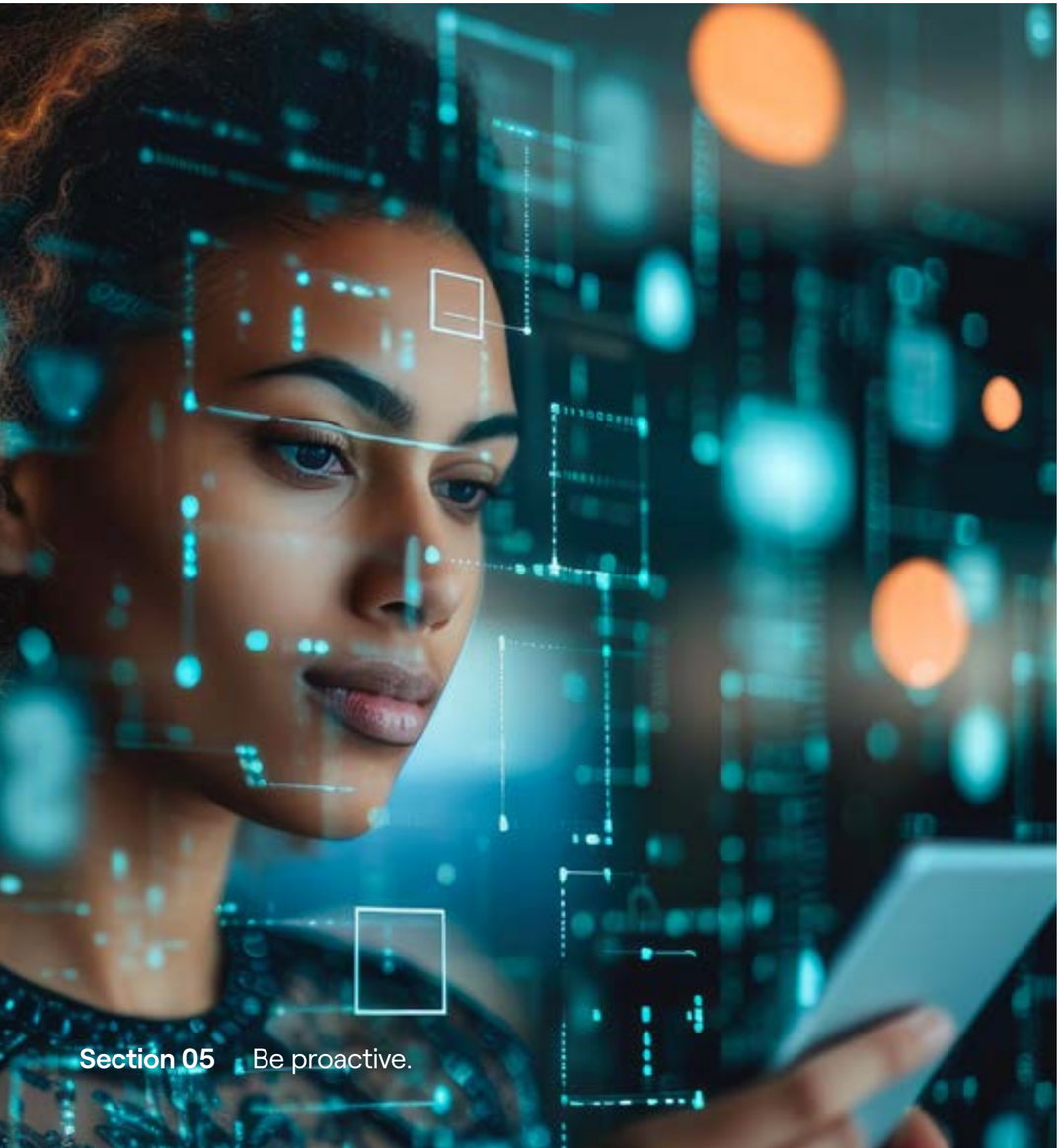
Regulatory changes highlight a clear focus on countering increasingly advanced fraud techniques, including synthetic identities, AI-driven biometric spoofing (e.g., deepfakes), the use of “mule accounts,” and social engineering attacks. This necessitates robust liveness detection and anti-spoofing capabilities.



Adopting international standards.

Countries are aligning with or explicitly requiring compliance with international security standards, such as ISO 30107-3 for presentation attack detection, FIDO Alliance biometric and identity verification (IDV) requirements. Validation by third party organizations and trusted test laboratories are being mandated to ensure the reliability and interoperability of identity verification technologies.

back to contents



Due diligence on technology and providers.

There is an increased regulatory expectation for financial institutions to conduct rigorous due diligence on their eKYC solutions and technology providers, including external independent assessments and continuous monitoring of performance metrics.

consult hyperion

back to contents

6. The challenge of supplier selection.

Even with clear criteria and a robust understanding of required solutions, the journey of selecting and qualifying an eKYC supplier is fraught with challenges for financial institutions (FIs).

consult hyperion

back to contents

Lack of internal expertise

Without the proper expertise to evaluate the complex technologies involved, FIs can underestimate risks or overestimate a supplier's capabilities.

Integration complexities

Solutions must integrate seamlessly with FI's intricate legacy systems or risk technical hurdles, unexpected costs, and project delays.

Vendor lock-in

Banks should avoid choosing a proprietary solution that leads to long term dependence. Instead, identify future-proof solutions with flexibility that enable them to evolve the offer as technologies develop and mature.

Evolving regulatory landscape

A compliant solution today may not be compliant tomorrow. FIs need to find partners who are proactive in adapting to new mandates.

Data security & privacy concerns

Entrusting sensitive customer data to a third-party requires rigorous due diligence in their security protocols, data handling practices, and compliance.

Underestimating operational risks

Predicting the operational impact of a new solution on customer journeys and internal processes is challenging without deep contextual understanding and regional insight.

Avoiding wasted investment

Investing heavily in a solution that performs poorly results in wasted resources and exposure to risk.
An inefficient or unqualified solution can eliminate benefits, turning an investment into a financial drain.

7. Key supplier selection criteria.

When selecting an identification and authentication solution supplier (or suppliers), a rigorous evaluation is essential to ensure the implementation aligns with specific objectives and requirements.

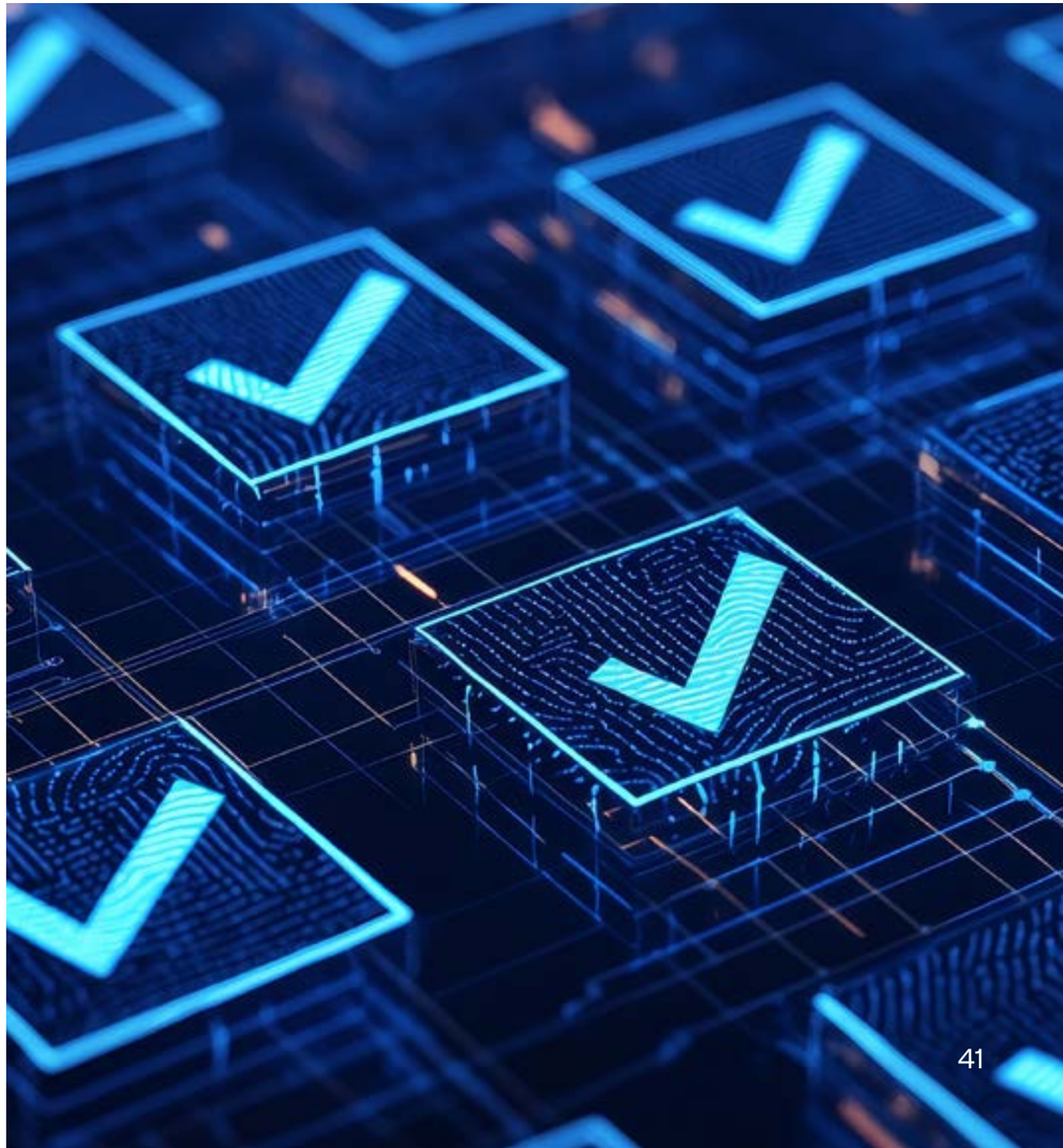
A high-level checklist might include:

Coverage: including geographical reach, functionality, future-proofing, adaptability to evolving requirements.

Quality: scrutinizing data sources for reliability and quality issues, assessing the effectiveness of de-duplication, matching and cross-referencing tools.

Efficiency: assessing automation, digitalization and customer interaction channels.

Support: examining SLAs, issues management, supplier stability and performance across operating systems.

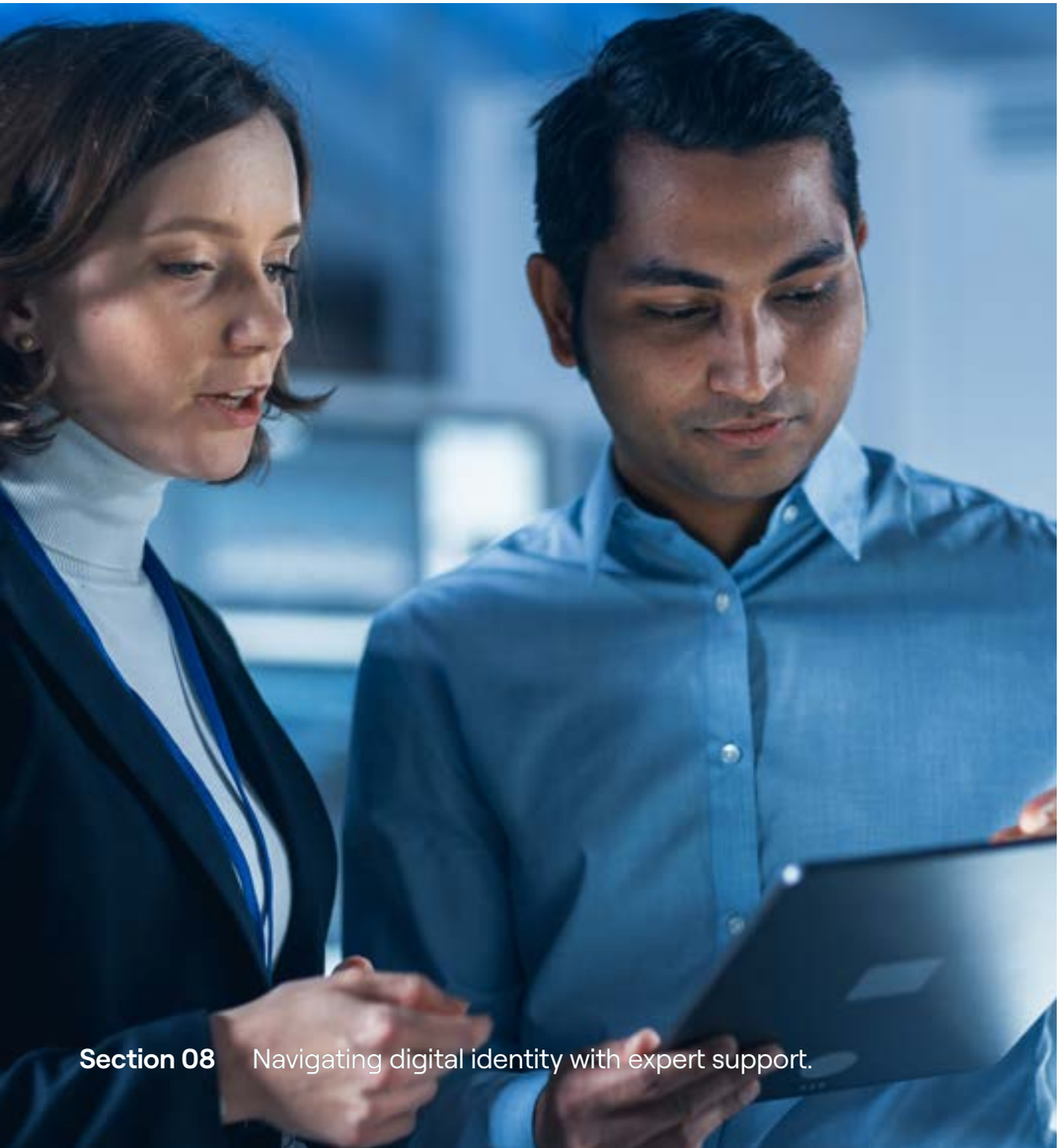


Maturity: evaluating the solution's track record, including testing methodologies, performance metrics and certifications.

Security: including attack resistance, fake or synthetic identity detection, account take-over resistance, integrated fraud detection and prevention, risk-based assessment mechanisms and more.

Compliance: adherence to Anti-Money Laundering (AML), Know Your Customer (KYC), Customer Due Diligence (CDD), and relevant personal data protection laws.

8. Navigating digital identity with expert support.



Navigating the treacherous waters of digital identity verification, fraud, and regulatory compliance requires more than just an internal review. Banks and financial institutions need reliable, knowledgeable, and neutral support to complete this critical journey.

An independent and knowledgeable consultant can provide:

- **Strategic guidance:** helping banks and financial institutions define an eKYC strategy that aligns with key business objectives, risk appetite, and regulatory obligations based on their customer portfolio and targeting roadmap.
- **Market intelligence:** providing up-to-date insights into both global and regional fraud trends, regulatory changes, and the competitive landscape of eKYC solutions.
- **Defining requirements:** translating multiple complex business and compliance needs into clear and tangible technical specifications for suppliers.
- **Vendor sourcing and vetting:** identifying potential suppliers, conducting initial assessments, and shortlisting candidates based on predefined criteria.
- **Contract negotiation:** assisting with the negotiation of service level agreements (SLAs), security clauses, and compliance guarantees.

A trusted testing partner plays an equally crucial role by offering:

- **Unbiased performance validation:** validating the accuracy, speed, and reliability of a solution under real-world conditions.
- **Security vulnerability assessment:** conducting penetration testing and security audits to identify any weaknesses in the solution's architecture, APIs, and data protection mechanisms.
- **Compliance verification:** independently assessing if the solution truly meets specific regulatory requirements.
- **Interoperability testing:** confirming that the solution can seamlessly integrate with existing IT infrastructure and third-party systems to ensure optimal customer experience.
- **Benchmarking:** providing comparative analysis of different solutions, offering objective data to support decision-making and ensuring the chosen solution is best-in-class.
- **Risk mitigation:** quantifying the operational, fraud, and compliance risks associated with different solutions, allowing decision makers to make informed choices that mitigate potential liabilities.

Work with an expert partner for a secure digital future

The pace of change is accelerating. Robust identity verification and user authentication are foundational tools helping financial institutions to manage customer onboarding and ongoing lifecycle management. Against the backdrop of a transforming threat landscape, however, financial institutions that stand still risk financial losses, reputational damage and the erosion for customer trust.

fime × consult hyperion
consulting by fime

back to contents

Combining Fime's accredited testing laboratory and Consult Hyperion's consulting expertise, our end-to-end service helps financial institutions navigate the complexities of strategic analysis, supplier selection and embrace the digital future with resilience and confidence.

Looking to select and deploy the best-in-class solution? Let's talk.

Share your challenge.

Our Fime experts are here to help you make innovation possible, from defining, designing to delivering and testing your products and services.

- visit fime.com
- or contact sales@fime.com

Making innovation possible.

Making the world work.

Consulting | Test Platforms | Testing Services