

The **Trust** Playbook:

2026 ready strategies for identity, trust & growth



IDnow.

Table of contents

Introduction

- The Trust Playbook Vision 2
- Compliance, Fraud, Technology and Trust Takeaways 4

Section 1: The Compliance Landscape in 2025 10–35

- How Businesses Must Rethink Identity Verification 10
- eIDAS 2 & The EU Digital Identity Wallet (EUDI Wallet) 11
- PSD3 & Payments Regulations: Redefining Trust in Digital Transactions 15
- AMLD6 & AMLR: Raising the Bar on Financial Crime Compliance 19
- UK, US & APAC: The Global Compliance Tightrope 21
- IDnow's Orchestration Identity & Trust Platform: Compliance at Scale 23
- Trust Services & QTSP Benefits 27
- Regulatory Guide 2025–2027 29
- Global Regulations Summary 30

Section 2: The Rising Fraud Threat in 2025 36–52

- Introduction to the Fraud Threat Landscape 37
- Identity Fraud 38
- The Deepfake Arms Race 40
- Synthetic Identities 42
- Account Takeover (ATO) 44
- APP Fraud & Social Engineering 46
- Internal Threats: Insider Fraud & Risks 48
- Why IDnow is Your Ultimate Defense Against Fraud 50

Section 3: The Technology Disruption in Digital Identity

53

- Why Businesses Must Stay Curious, Not Just Compliant 54
- AI & Machine Learning in Identity Verification 55
- Digital Wallets & Verified Electronic Attributes 56
- Large Language Models & Generative AI 58

Section 4: The Essential Tech Guide

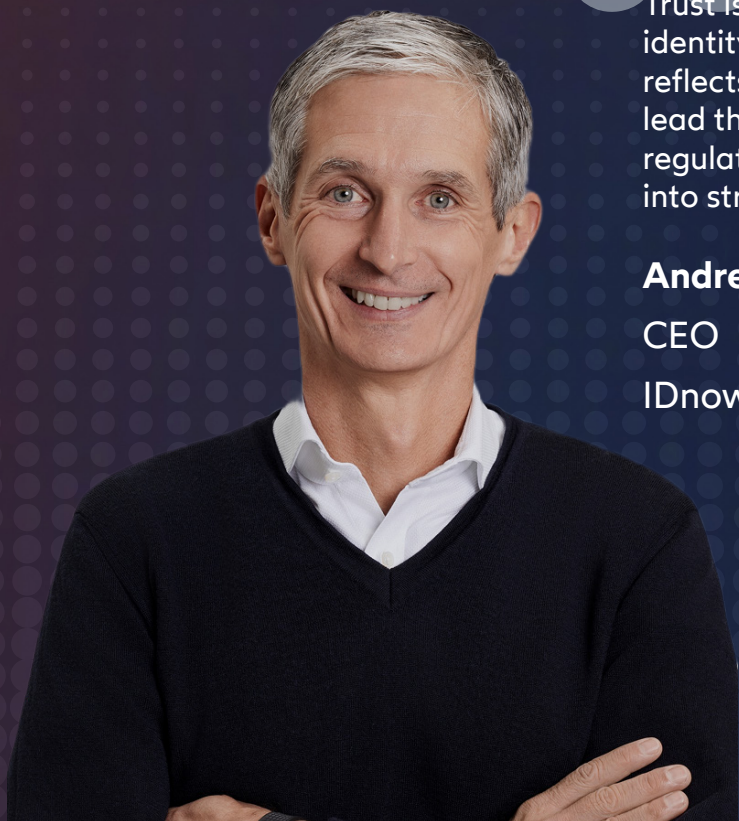
61–63

- Your Future-Ready Identity Stack in 2025 61
- IDnow's AI + Human Hybrid Model 62
- Checklist & Key Takeaways for Tech-Driven Compliance 63

Building **trust** in the age of identity disruption

2025 marks a turning point for digital identity. As regulations tighten and fraud risks intensify, businesses face growing pressure to stay compliant, secure, and competitive - all at once. But what if the real opportunity isn't just in surviving this change, but in leading it?

This playbook explores how forward-thinking organisations can turn today's compliance chaos into tomorrow's competitive edge. From eIDAS2 and the EU Digital Identity Wallet to the rise of AI, decentralised identity, and generative fraud, we unpack what's changing and what to do about it.



Trust is the new currency in a world where identity is being redefined. This playbook reflects our vision for how businesses can lead through disruption, not just by meeting regulatory demands, but by turning them into strategic advantage.

Andreas Bodczek

CEO

IDnow



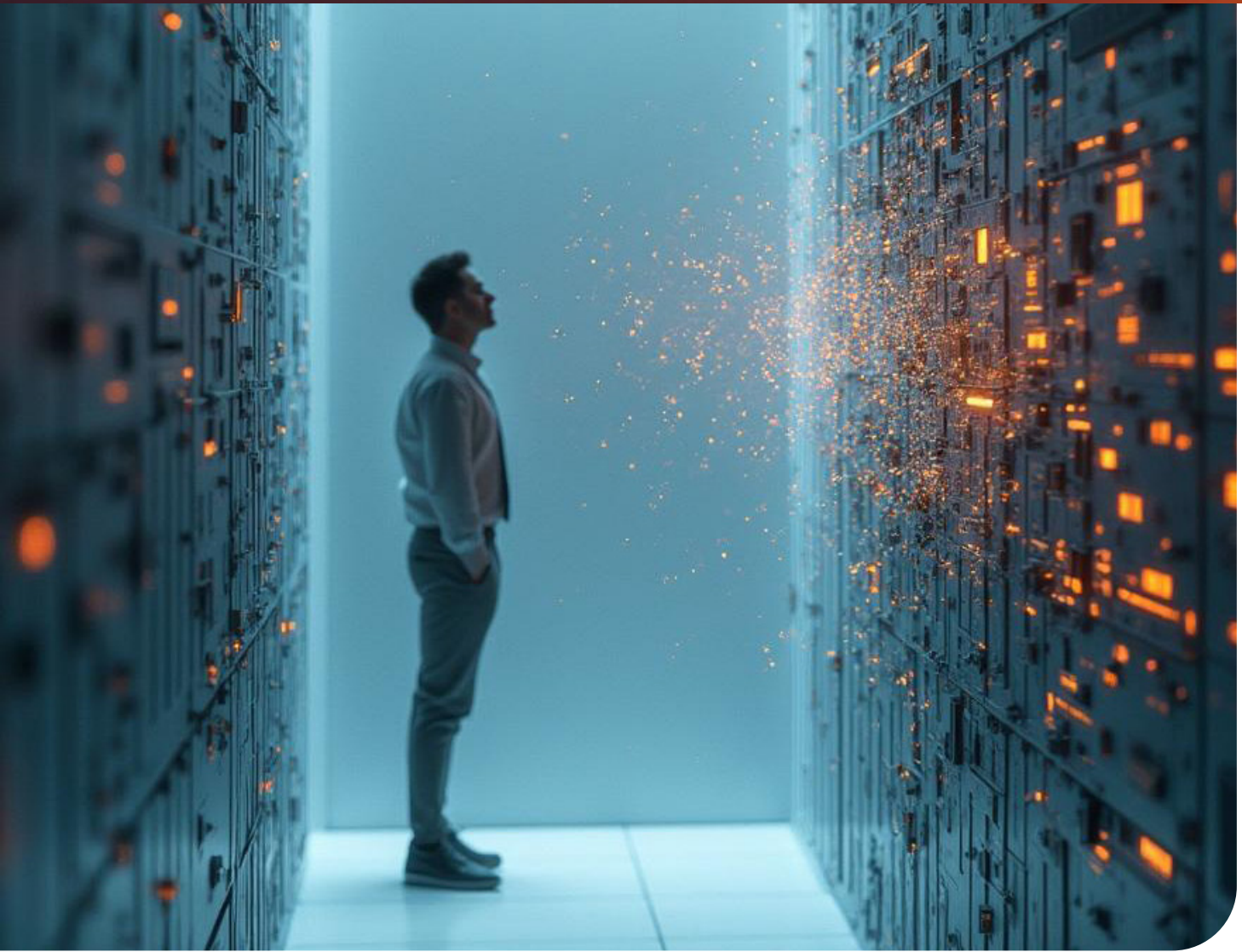
1. The **compliance** crunch is coming

Regulations like eIDAS2, AMLR, and PSD3 are reshaping the rules of engagement for identity verification and fraud prevention. The introduction of the EU Digital Identity Wallet promises frictionless onboarding, but only for those who can integrate fast and stay audit-ready. The cost of inaction? Missed growth opportunities, non-compliance penalties, and exposure to advanced fraud.

The takeaway:

Compliance isn't just a checkbox, it's your license to operate and a chance to streamline trust, onboarding, and security in one move.





2. The **fraud** threat is scaling fast

Fraud in 2025 is faster, smarter, and harder to stop. Deepfakes, synthetic identities, and AI-driven scams are slipping past outdated defences at every stage of the customer journey. Learn how to fight back with real-time, adaptive fraud prevention.

The takeaway:

Waiting for the next guideline isn't a strategy. To stay ahead, you must be curious, not just compliant.

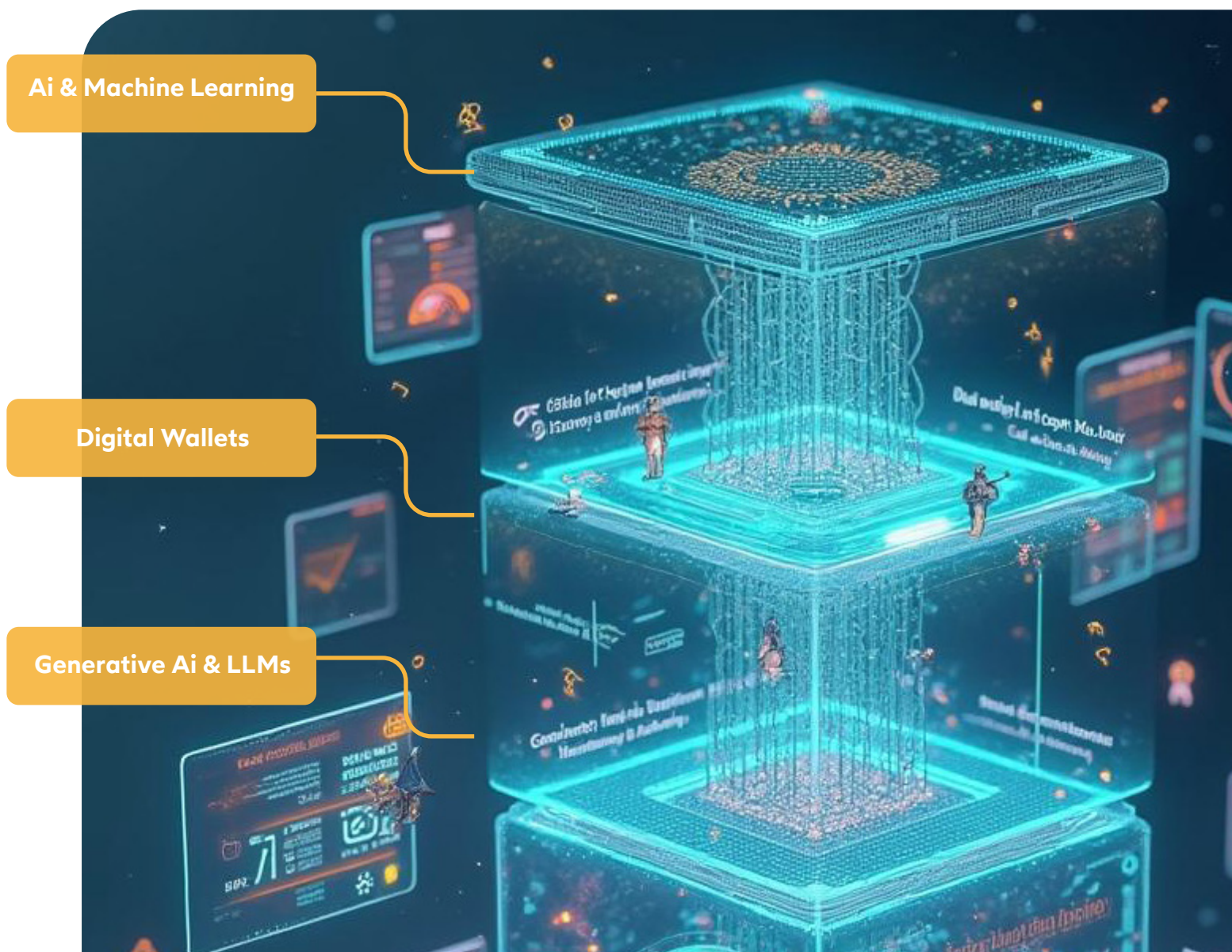
3. The new **trust** stack is here

The identity infrastructure of tomorrow is modular, scalable, and smart. At its core are three transformative technologies:

1. AI & Machine Learning for smarter, explainable fraud detection
2. Digital Wallets & Decentralised Identity for user-controlled onboarding
3. Generative AI & LLMs for both defensive innovation and evolving threats

The takeaway:

Your tech stack must evolve as fast as the threat landscape. Static defences are dangerous ones.



4. Why IDnow is redefining trust.

IDnow Trust Platform is built for this new world. It orchestrates identity, fraud, and compliance in one adaptive, AI-powered platform future-proofing your customer journeys while keeping regulators satisfied. Whether you need to verify an identity once or continuously monitor trust over time, IDnow enables you to do both, with security and scale baked in.

And trust doesn't stop at identity verification. Through our partnership with IDnow Trust Services AB, a Qualified Trust Service Provider (QTSP), we offer seamless access to eIDAS2-compliant Qualified Electronic Signatures (QES), trust services, and digital identities, helping you meet the highest standards of assurance and legal validity across Europe.

This aligns with our new vision:

To be the gateway to a secure digital trust ecosystem where identity isn't just verified but continuously enriched and secured - setting a new standard of trust that drives lasting competitive advantage in the global digital economy.





The takeaway:

Trust is no longer a feature - it's your foundation. And IDnow turns it into your biggest competitive advantage.

And our mission is clear:

We transform trust into the most powerful asset in the digital world, empowering enterprises with AI-driven, SaaS-based identity solutions that deliver scalable security, adaptive compliance, and real-time fraud prevention.

Ready to lead, not follow?

This playbook is your guide to navigating the new identity frontier - confidently, compliantly, and competitively. Whether you're building your future roadmap or responding to regulatory deadlines, IDnow is here to help.

- ☐ **Get early access updates** on the IDnow Trust Platform
- ☐ Talk to our **product experts about your** identity strategy

Section 1:

The compliance landscape in 2025

•



How businesses must **rethink** identity verification to stay ahead.

If digital identity is the key to trust, then compliance is the framework that shapes the lock. In 2025, businesses face a shifting regulatory landscape that's not just raising the bar for identity verification, it's redefining what's possible.

Staying compliant is no longer just about ticking boxes; it's about aligning with evolving regulations to build secure, seamless, and trustworthy digital experiences.

Across Europe and beyond, major regulations like eIDAS2, AMLR, and PSD3 are reshaping how businesses verify customers, prevent fraud, and protect transactions. These aren't just bureaucratic updates; they redefine the very foundation of how companies onboard users, process payments, and prevent financial crime.

Take eIDAS2 and the EU Digital Identity Wallet (EUDI Wallet), for example, it promises to streamline digital identity across Europe and also introduces new fraud risks and interoperability challenges. Meanwhile, PSD3 and AMLR are raising the bar for security and anti-fraud measures, making compliance a high-stakes game.

The challenge? Balancing security, user experience, and fraud prevention while keeping up with evolving requirements.

The opportunity? Turning compliance into a competitive advantage, by delivering faster, safer, and more trusted digital interactions.

Let's break down what's changing, what it means for businesses, and how companies can turn compliance from a headache into a competitive advantage.

eIDAS 2 & The EU digital identity wallet: The future of digital identity in europe

Imagine a world where proving who you are online is as simple as unlocking your phone. No more remembering dozens of passwords. No more scanning documents and waiting for approvals. That's the promise of eIDAS 2 and the EU Digital Identity Wallet (EUDI Wallet), a government-backed digital identity system designed to streamline verification across Europe.

By 2026, every EU citizen will be able to store and share verified credentials such as their ID, bank details, and even medical records via a digital wallet. And by 2027, businesses in regulated industries (finance, mobility, telecom, gambling) must accept the EUDI Wallet as a valid form of identity verification.



Why this matters

For Businesses:

Global organizations will need to integrate digital wallets into onboarding and authentication flows. This means rethinking how customers sign up, verify their identity, and access services.

For Customers:

Forget long KYC processes and having to identify yourself every time you want to open a new account or register for a service. Wallets will enable instant verification. Need to open a bank account? Rent a car? Sign up for a gaming platform? Just share your verified identity details.

The Challenges.

Fraud risks:

Digital wallets will simplify authentication, but they also create new attack opportunities for fraudsters. Can businesses trust that a wallet-stored identity is legitimate?

Interoperability woes:

Every country will develop its own version of the wallet, but will they work seamlessly across borders? A French citizen should be able to open a German bank account with the same ease as a local citizen.

Integration complexity:

Businesses must redesign onboarding workflows to support wallet-based authentication, ensuring compatibility with existing KYC systems.

The Opportunities.

Faster onboarding & better user experience:

Customers can reuse their verified identity instantly, reducing drop-off rates and boosting conversion.

A borderless identity ecosystem:

Individuals can access services across Europe without repeating identity checks, unlocking true digital mobility.

Stronger compliance with less effort:

Businesses can meet KYC and AML requirements using pre-verified identity credentials, reducing compliance costs.



“

The EUDI Wallet is a game-changer, but businesses must prepare now. IDnow Trust Platform ensures seamless wallet verification, fraud checks, and compliance automation, turning a regulatory requirement into a competitive advantage.










Armin Berghaus

Chief Technology and Security Officer
IDnow

National wallets across Europe

As part of the EUDI initiative, several EU Member States are developing their own national digital identity solutions, which will be integrated into the pan-European EUDI Wallet framework. Here are some examples of the national wallets:

	Austria	ID Austria
	Belgium	itsme
	Denmark	MitID
	Finland	FTN (Finnish Trust Network)
	France	France Identité” app, and IN Groupe Wallet
	Germany	Personalausweis
	Estonia	ID-kaart and Mobiil-ID

These wallets will be connected through the IDnow's Identity & Trust Platform, allowing businesses to seamlessly manage identity verifications across all 27 EU countries without needing to implement 27 separate integrations. The Identity & Trust Platform's single API integration provides access to these various wallets, supporting businesses as they navigate the complexities of compliance, fraud prevention, and cross-border identity verification.



PSD3 & payment regulations: redefining trust in digital transactions

Imagine a payment experience where fraud is detected in real-time without blocking legitimate customers. That's the future promised by PSD3 - the next evolution of the EU's Payment Services Directive - designed to bring stronger security and a smoother customer experience to every digital transaction.

As fraudsters grow more sophisticated and customer expectations rise, PSD3 signals a shift from basic fraud prevention to intelligent, proactive protection - without the friction that causes abandoned carts and lost revenue.

Why this matters

For Businesses:

Payment service providers, fintechs, and merchants must rethink how they verify users and manage fraud. Manual checks and fragmented systems won't cut it anymore.

For Customers:

They expect seamless, real-time payments - but only if their personal and financial data is protected at every step.

What's Changing

- 1. Stronger KYC & Identity Checks:** Stricter onboarding requirements for merchants, payment providers, fintechs and platform providers.
- 2. Transparency in Cross-Border Payments:** More clarity, speed, and security for customers sending or receiving funds across the EU.
- 3. Stronger Consumer Protections:** Companies will need to prove they're actively protecting customers from fraud and unauthorized transactions.

The Challenges.

Friction vs. Security:

How do you reduce fraud without increasing onboarding friction?

Evolving Threats:

Fraudsters are shifting tactics, PSD3 demands dynamic, ongoing protection.

Proof of Protection:

Regulators want evidence that your systems truly protect users.

The Opportunities.

Reduced False Positives:

Smarter fraud systems mean fewer blocked payments and happier customers.

Frictionless UX:

Fast, secure, and seamless identity checks embedded directly into the payment flow.

Growth-Ready Compliance:

Future-proof your payments setup for ongoing EU-wide regulatory changes.



“

The goal of PSD3 is clear, better security without breaking the payment experience. Providers who embed smart identity solutions will not only comply, they'll gain a competitive edge



Armin Berghaus

Chief Technology and Security Officer
IDnow

Who	What's Changing	Compliance Actions	Why It Matters
Merchants	Must adopt robust identity verification for onboarding and ongoing user management.	Implement real-time identity verification (e.g. eIDV), verify beneficial owners (for KYB), keep audit logs.	Prevent misuse of platforms for fraudulent payments or money laundering.
Payment Providers	Required to integrate dynamic, risk-based KYC/ KYB processes.	Use tiered verification based on risk level, monitor transactions continuously, report suspicious activity.	Meet stricter AML obligations and protect end-to-end payment flows.
Fintechs	Need to implement stronger identity checks and user verification at scale.	Automate KYC onboarding with biometric checks, liveness detection, and fraud screening tools.	Maintain compliance without scaling up manual review teams.
Platform Providers	Must verify both buyers and sellers with consistent, auditable identity checks.	Require ID checks for all users, integrate watchlist/ PEP screening, maintain user identity data securely.	Avoid platform misuse and enable compliant payments across user types.
Banks	Stricter onboarding and authentication requirements for new and existing customers.	Re-authenticate legacy users, enable multi-factor authentication, implement customer due diligence (CDD) updates.	Prevent account takeover and comply with evolving AML directives.
Mobility Providers	Must validate user identity for payment and platform usage.	Verify ID at account creation, especially for payment-linked services; enable frictionless KYC flows via mobile.	Ensure rider and driver safety, prevent payment abuse, and enable PSD3-compliant transactions.
Telecommunications Companies	Required to enhance SIM registration and mobile payment identity checks.	Implement ID verification during SIM issuance, cross-check payment-linked accounts, monitor for SIM swap fraud.	Protect users from identity theft and fraudulent mobile payments.
Gaming & Gambling Operators	Stricter KYC for player onboarding and transactions, especially for cross-border users.	Verify identity, age, and source of funds; perform ongoing risk assessments; comply with AML and PSD3 reporting.	Meet cross-border regulatory obligations and prevent fraud in real-money platforms.

AMLD6 & AMLR: raising the bar on financial crime compliance

The EU's fight against money laundering and terrorist financing is reaching a new level of intensity with AMLD6 (6th Anti-Money Laundering Directive) and the new AMLR (Anti-Money Laundering Regulation). Together, they mark a shift from reactive, box-ticking compliance to real-time, risk-based monitoring, and with much higher stakes for businesses.

What's the Difference?

1. AMLD6 is a directive, setting minimum standards for EU member states to transpose into national law. It expands criminal liability and harmonizes key definitions.
2. AMLR, by contrast, is a regulation immediately binding across all member states setting unified, stricter rules for KYC, transaction monitoring, and CDD (Customer Due Diligence). It eliminates national divergence by standardizing AML requirements across the EU.

Why this matters

For regulated businesses:

The pressure to detect and prevent financial crime in real time is higher than ever and penalties for non-compliance are steep.

For high-risk industries:

Crypto exchanges, neobanks, iGaming and fintech platforms face enhanced due diligence and supervision.



Key Changes

- 1. Corporate liability:** Under AMLD6, your business can be criminally prosecuted for failing to prevent money laundering, even if it's done by a third party on your platform.
- 2. Real-time risk monitoring:** AMLR demands dynamic, ongoing assessments, not static, once-off KYC.
- 3. Crypto in focus:** Virtual asset providers must comply with full AML standards, including beneficial ownership checks and sanctions screening.

The Challenges.

Legacy Systems: Many companies still rely on fragmented AML tools not built for real-time monitoring.

Operational Overload: Continuous due diligence can strain already stretched compliance teams.

Cross-Border Consistency: Global players must meet both EU and local AML rules in each market.

The Opportunities.

Automated Risk Analysis: Machine learning-driven fraud signals and behaviour analysis for better threat detection.

End-to-End KYC to KYT: Verify identities (KYC) and monitor transactions for fraud (KYT) in one streamlined solution.

Stronger, Smarter Compliance: Less manual intervention, fewer errors, better auditability.

UK, US & APAC: The global compliance tightrope

How Economic Crime Plans and New AML Laws are reshaping identity requirements worldwide.



UK Economic Crime Plan 2.0: The UK doubles down on dirty money

The UK is tightening its grip on financial crime with Economic Crime Plan 2.0, increasing fines for AML breaches and ramping up scrutiny of fintech, crypto, and high-risk sectors.

Tougher KYC expectations for digital platforms

Faster enforcement and bigger penalties for compliance failures

Increased public-private data sharing to combat fraud and laundering

Why It Matters: The UK's approach is more aggressive, especially post-Brexit. Businesses operating in or through the UK will need enhanced AML controls, documentation, and reporting capabilities.



U.S. FinCEN Beneficial Ownership Rule: ending the shell game

- As part of the U.S. Corporate Transparency Act, this rule requires most businesses to report their true beneficial owners to FinCEN, dramatically increasing transparency around shell companies and anonymous ownership.
- Impact on onboarding corporate clients and legal entities
- More due diligence expected for high-value transactions
- Cross-border companies must adapt U.S.-facing KYC workflows

Why It Matters: Companies serving U.S. markets need systems that can handle granular ownership data and audit trails.



APAC's KYC & AML Shift: digital identity goes mainstream

- APAC is moving fast on digital compliance, with countries like Singapore, Australia, Hong Kong, and China implementing stricter AML rules and mandating digital KYC.
- Singapore's Monetary Authority of Singapore now mandates digital ID verification and real-time transaction monitoring
- Australia's new AML consultation focuses on crypto, remittance, and gaming providers
- China is cracking down on fintech fraud and tightening license requirements

Why It Matters: Global businesses can't take a "one-size-fits-all" approach. Identity and compliance platforms must be flexible, adaptable, and localised.



How IDnow can turn your compliance challenges into your competitive advantage:

Integrating just one digital wallet into your systems is no small feat, especially when each country brings its own unique set of regulatory nuances, technical requirements, fraud threats, and user expectations. Now imagine doing that 27 times, at scale, across Europe. That's the reality many businesses will face as the EUDI Wallet rollout accelerates.

That's where IDnow Trust Platform comes in. It is designed to be your single gateway to trust, offering a future-proof, flexible, and secure way to support eIDAS2, national eID schemes, and the upcoming EU Digital Identity Wallets, without the burden of building and maintaining 27 separate integrations. And it's not just about digital identity. The same infrastructure that helps you onboard and verify EUDI Wallet users also helps you meet the evolving demands of AML, KYC, and payments regulations globally.

By partnering with IDnow Trust Services AB a Qualified Trust Service Provider (QTSP), IDnow provides the highest level of assurance when it comes to digital Trust services. Our services are fully compliant with eIDAS2, offering you not just compliance but a competitive edge when it comes to managing trust, security, and identity across Europe.

One API to connect them all

With a single API integration, you'll unlock every major identity verification path in Europe, from EUDI Wallets and national eID schemes to AMLR-compliant, document-based verification.

This gives you the flexibility to:

Seamlessly integrate with eID schemes such as the France Identité" app, ID Austria, Belgium's itsme or Germany's Personalausweis

Add or update wallet connections without the hassle of additional integrations

Integrate risk-based KYC workflows tailored to PSD3 or AMLR expectations

Trigger enhanced due diligence or beneficial ownership checks based on customer profile or geography

Onboard users across all 27 EU member states using their existing EUDI wallets

Think of it as a 'plug once, scale everywhere' model, that will free your team from repetitive technical work and let you focus on growth.



Custom workflows for every business need

Every business is different, different markets, different risk thresholds, different customer journeys. That's why we designed the IDnow Trust Platform to be highly customizable, with flexibility at its core. Whether you're operating in financial services, gaming, or mobility, the Identity & Trust Platform empowers you to design and customize your identity verification and compliance workflows to meet your specific requirements, without the need for heavy IT involvement. Easily design and customize your identity verification user and compliance flows our advanced technology and adaptable prompts. With the IDnow Trust Platform you can:

Design and Customize your identity verification and compliance workflows using pre-built, modular templates tailored to your business needs.

Reuse proven workflow blueprints across countries or compliance requirements, saving time on workflow planning, localization, and compliance and onboarding optimisation testing

Enjoy the flexibility and control of a bespoke solution with the speed, scalability, and reliability of a SaaS platform

Trigger real-time fraud detection and continuous monitoring in line with AMLR and PSD3 requirements

Create highly flexible workflows by adjusting the sequence of document checks, biometric verifications, fraud detection layers, and digital wallet interactions, based on geography, customer segment, or risk profile.

Automate AML screening rules, including sanctions, PEP, and adverse media checks

Enjoy the benefit of GenAI integrated into our Studio and leverage native LLM (Large Language Models) or SLMs (Specialized Language Models) within the Identity & Trust Platform for seamless flow generation or to create customizable agentic modules. These models can address complex problems, such as tailored checks, without the need for custom algorithms, enabling faster and more dynamic workflow design.

Whether you're launching in one market, 27 or more, the IDnow Trust Platform gives you the agility to move fast and stay compliant.

Granular results + audit-ready compliance

Auditors love paperwork, you probably don't. But with IDnow, you can breathe easy, we've built compliance into the very DNA of the IDnow Trust Platform, so you don't have to chase logs, piece together user journeys, or worry about falling short when the regulators come knocking. Whether you're preparing for an internal review or a full-scale audit, everything you need is already documented, organised, and ready to share. With our Identity & Trust Platform you get:

A complete, secure log of every identity verification step, biometric check, fraud rule match, and wallet interaction, all timestamped, encrypted, and stored in line with GDPR and regulatory requirements

Instant export of PDF audit trails that are pre-structured for eIDAS2, AMLR, PSD3, FinCEN or local regulatory reviews, no formatting, filtering, or stress required

Granular decisioning results for every verification: pass, fail, manual review, with detailed reason codes that offer full transparency into what happened and why

Monitoring reports for AMLD6-required criminal liability thresholds



"Think of it as your digital paper trail, automated, reliable, and always one step ahead of compliance." Explains Michael Soliman. "With the IDnow Trust Platform, our customers will be able to demonstrate to auditors exactly how and when each identity was verified, no grey areas, no guesswork."

A launchpad for cross-border growth

eIDAS2 isn't just a compliance hurdle, and neither are PSD3, AMLR, or the UK's Economic Crime Plan 2.0. Each represents both a regulatory challenge and a strategic opportunity for businesses looking to scale across borders while building trust at every touchpoint.

While many companies focus on ticking regulatory boxes, the real advantage lies in creating future-proof onboarding and compliance frameworks that can adapt as regulations shift while using the EUDI Wallet as a trusted, pan-European identity gateway and a launchpad for European expansion. With millions of users soon equipped with reusable digital IDs and global regulators tightening the net, businesses that integrate early can unlock faster onboarding, reduced fraud risk, and seamless access to customers across 27 countries.

With the IDnow Trust Platform, you're not just meeting regulatory requirements, you're positioning your business to scale quickly, reduce operational costs, and offer a best-in-class onboarding experience, no matter where your users are in Europe.

With the IDnow Trust **Platform you can:**

Accept customers from across the EU with a verified wallet in seconds

Work with a single trusted supplier, avoiding the pain of managing multiple local vendors

Build risk-based onboarding flows that adapt dynamically based on user behaviour, region, or product

Expand into new European and international markets faster, confident you're aligned with EU, UK, US, and APAC KYC, AML, and payments regulations

Deliver seamless user experiences in every language and jurisdiction from a single, unified platform

Confidently support multi-region compliance strategies that evolve with laws like PSD3, AMLR, the UK Economic Crime Plan, the U.S. FinCEN Beneficial Ownership Rule, and APAC's Digital KYC mandates

IDnow.



The IDnow Trust Platform removes the barriers to operating pan-European and global services. It's our foundation for scaling trust."

Uwe Stelzig,
Managing Director DACH
IDnow



Trust Services & QTSP

Benefits: ensuring compliance and security

With our partnership with IDnow Trust Services AB, IDnow provides the highest level of assurance in digital Trust services, ensuring compliance with the latest regulatory standards like eIDAS2, PSD3, and AMLR. In the fast-evolving landscape of digital identity and fraud prevention, trust services play a pivotal role in securing transactions and protecting both businesses and their customers. Here's how using qualified trust services from IDnow Trust Services AB helps you navigate regulatory complexities and gain a competitive edge:

1. Regulatory compliance at the core:

By using IDnow Trust Services AB, you're assured of compliance with the eIDAS2 Regulation (Electronic Identification and Trust Services for Electronic Transactions), which is foundational for Digital Identity Wallets and other trusted online services across Europe. As a QTSP, IDnow Trust Service's services are audited and verified to meet stringent EU regulations, ensuring that every digital identity verification is legally recognized and secure. The roadmap for IDnow Trust Services also includes advanced eIDAS2 trust services such as issuance of Qualified Electronic Attribute Attestations (QEAA), issuance of Public Electronic Attribute Attestations (pub-EAA), qualified archiving, and qualified preservation.

2. Ensuring alignment with ETSI standards

In addition to being a Qualified Trust Service Provider (QTSP), IDnow's identity verification products are already compliant with ETSI TS 119 461 v1.1.1 the European technical specification for identity proofing and will be updated to comply with the upcoming ETSI TS 119 461 v2.1.1

standard by 2026. This ensures that our services remain at the forefront of eIDAS2 compliance, offering peace of mind that your onboarding and identity verification flows are fully aligned with both current and future EU requirements.

3. Enhanced security for digital transactions:

Trust services ensure the highest levels of security for online transactions. Qualified electronic signatures (QES), electronic seals, and time-stamping services offer verifiable, tamper-proof digital records that provide legal assurance and protect businesses from fraud and identity theft. This guarantees your customers that their data is secure and handled with the utmost integrity. Qualified certificates issued by IDnow Trust Services are used for the remote creation of QES. The QES are legally binding and can therefore be applied on contracts.

4. Simplified cross-border compliance:

Navigating the intricacies of cross-border regulations can be challenging. As a QTSP, IDnow Trust Services' services provide a

uniform standard of trust that aligns with both eIDAS2 and PSD3, making it easier for you to extend your services across the EU and beyond, while maintaining full compliance with local regulatory frameworks. This cross-border compliance is key as the EUDI Wallet and other digital identity services expand across Europe. Notably, IDnow Trust Services is the first QTSP in the EU to implement the OTP-less remote signing flow, enabled by a recent standardization change at ETSI, simplifying the user experience while remaining fully compliant.

5. Future-proofing your compliance strategy:

With trust services integrated into your workflow, IDnow Trust Services QTSP status ensures that your systems are prepared for future regulatory changes, including the EU Digital Identity Wallet rollout and tightening fraud prevention laws. Qualified certificates issued by the IDnow QTSP are used for remote creation of QES. The QES are legally binding and can therefore be applied on contracts.

6. Streamlined digital identity verification:

IDnow Trust Services AB simplify and streamline the verification process, making it easier for you to onboard customers quickly, securely, and in compliance with regulations like AML and KYC. The ability to integrate trusted, verified digital identities into your workflows allows for faster, more efficient user journeys, while still ensuring the highest standards of fraud prevention and compliance.

Conclusion:

In Section 1: The Compliance Landscape in 2025, we've outlined the key regulations shaping digital identity and fraud prevention, including eIDAS2, AMLR, ALMD6, PSD3, and others. We've highlighted critical deadlines, compliance requirements, and the wider impact on your business.

Now, we're excited to present our Essential Guide, a concise snapshot of everything you need to know and do to stay ahead. Perfect for sharing with your colleagues, this guide offers practical steps to ensure you're fully prepared.



Regulatory guide 2025–27

Key digital identity & compliance milestones at a glance

Timeline for eIDAS2 / EUDI Wallet:



- Apr 2024- Regulation approved
- Nov 2026- Wallets available
- Nov 2027- Mandatory business acceptance



PSD3 (Payments Regulation)

- 2025- Proposal phase

AMLD6 / AMLR

- July 2027- AMLD6 transposition deadline
- July 2027 - AMLR rules become fully binding



UK Economic Crime Plan 2.0

- 2023–2026- Implementation window

Industries Affected

Financial Services (FS)

Telecommunications

E-commerce

Legal & Accounting Firms

Public Sector / Government

Crypto / VASPs / Remittance



U.S. FinCEN Rule

- Jan 1, 2024- Rule effective
- Jan 1, 2025- Deadline for existing entities
- 30-day ongoing reporting

Key Pillars:

- Beneficial ownership reporting
- Legal/operational risks
- Continuous KYC updates

APAC Region Map:



Singapore

Monetary Authority of Singapore (MAS)



Australia

Australian Transaction Reports and Analysis Centre (AUSTRAC)



China

People's Bank of China (PBoC)

1. eIDAS2 and the EU Digital Identity Wallet (**EUDI Wallet**)

Key dates:

June 2025 – eIDAS2 regulation was approved and published by the EU

November 2026 – Wallets will become available

November 2027 – Mandatory business acceptance

Industries Impacted:

Financial Services (FS)

E-commerce

Public Services

Telecommunications

Regulator:

European Commission, EU Council and the EU Parliament.

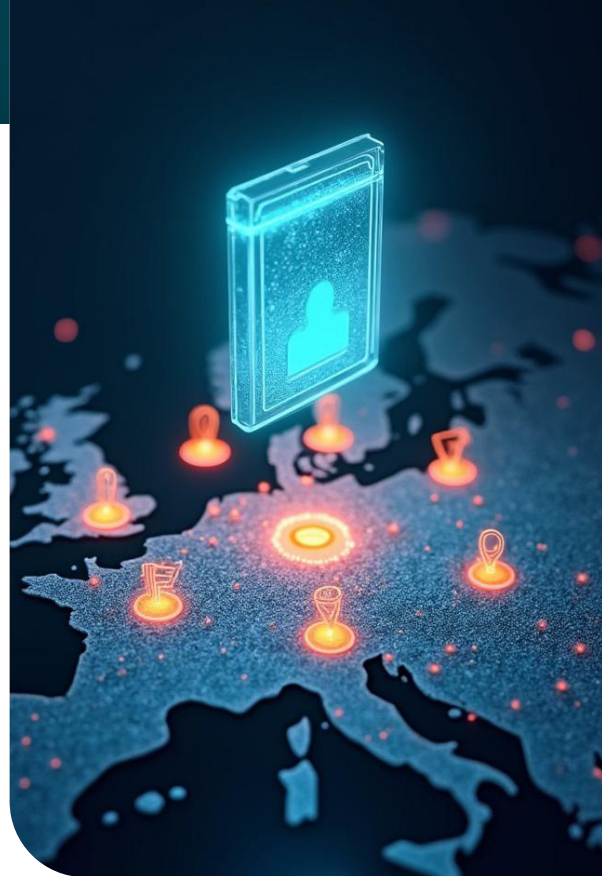
Top 3 impacts for businesses & customers:

1. **Enhanced User Experience:** Simplifies user authentication across services, reducing friction in customer interactions.
2. **Operational Efficiency:** Streamlines KYC processes, lowering onboarding times and associated costs.
3. **Cross-Border Interoperability:** Facilitates seamless digital interactions across EU member states, expanding market reach.

Key Actions: Immediate **Next Steps** for Compliance:

- **April 2024 – start compliance prep**
- Assess how eIDAS2 impacts onboarding and authentication
- Review your current IDV and KYC processes
- Engage partners (e.g., IDnow) to explore integration
- Begin planning to avoid disruption
- **November 2026 – wallets go live**
- Member states must offer EUDI Wallets
- Businesses should be in testing/pilot phase
- Ensure systems can process digital IDs
- Align with security and fraud prevention standards
- Integrate into existing KYC workflows
- **November 2027 – mandatory business acceptance**
- Accept EUDI Wallet credentials as valid ID
- Fully integrate into onboarding/authentication flows
- Ensure compliance with eIDAS2, AMLR, etc.
- Apply fraud prevention (e.g., spoofing/synthetic ID checks)

2. Payment Services Directive 3 (PSD3) and Payments Regulation Shifts



Deadline:

Late 2025: PSD3 and PSR adopted

Mid-2027: PSD3 transposed; PSR applies

From Q1 2027: Full EU compliance required

Industries Impacted:

Financial Services (FS)

Payment Service Providers

E-commerce

Regulator:

European Commission

Top 3 Impacts for Businesses & Customers:

- 1. Strengthened Consumer Protection:** Introduces enhanced security measures for electronic payments, increasing customer trust.
- 2. Innovation in Payment Services:** Encourages the development of new payment solutions, fostering competition and innovation.
- 3. Regulatory Compliance Burden:** Imposes additional compliance requirements, necessitating updates to existing processes and systems.

Key Actions: Immediate Next Steps for Compliance:

- **Monitor Legislative Progress:**
- Keep abreast of PSD3 developments and assess potential impacts on operations.
- **Engage in Industry Dialogue:**
- Participate in consultations and provide feedback to shape the directive's final form.
- **Prepare for Implementation:**
- Begin preliminary assessments of necessary system and process changes to meet anticipated requirements.

3. Anti-Money Laundering Regulation (AMLR) and Anti-Money Laundering Directive 6 (AMLD6)

Deadline:

AMLD6 Transposition
Deadline: 10 July 2027

AMLR Implementation:
Ongoing, with various
provisions coming into
effect between 2025 and
2027

Industries

Impacted:

Financial Services (FS)

Crypto Asset Providers

Legal and Accounting
Firms

Regulator:

European Commission.

Top 3 Impacts for Businesses & Customers:

1. **Expanded Criminal Liability:** Broadens the scope of predicate offenses and holds companies accountable for AML breaches.
2. **Enhanced Due Diligence:** Imposes stricter KYC requirements, affecting customer onboarding and monitoring processes.
3. **Increased Regulatory Scrutiny:** Subjects businesses to more frequent audits and higher penalties for non-compliance.

Key Actions: Immediate Next Steps for Compliance:

- **Review AML Policies:**
 - Update internal policies to align with AMLD6 and AMLR provisions.
- **Train Staff:**
 - Conduct comprehensive training programs on new AML obligations and procedures.
- **Implement Monitoring Systems:**
 - Invest in advanced transaction monitoring tools to detect and report suspicious activities effectively.

4. UK Economic Crime Plan 2.0



Deadline:

Mar 2023: Plan 2.0 launched

2024: Crypto regulation introduced

2024–25: Multi-Agency Cell set up

2025: NECC expanded

Mar 2026: Implementation review & Plan 3.0 prep

Industries

Impacted:

Financial Services (FS)

Real Estate

Legal and Accounting Firms

Regulator:

UK Government

Top 3 Impacts for Businesses & Customers:

- Enhanced AML Measures:** Introduces stricter AML controls, impacting compliance obligations for businesses.
- Increased Transparency:** Mandates greater disclosure of beneficial ownership, affecting corporate structures.
- Stronger Enforcement:** Allocates more resources to investigate and prosecute economic crimes, increasing legal risks.

Key Actions: Immediate Next Steps for Compliance:

- Evaluate Compliance Frameworks:**
 - Assess and strengthen existing AML policies and procedures.
- Enhance Due Diligence:**
 - Implement more rigorous customer and transaction screening processes.
- Engage with Authorities:**
 - Collaborate with regulatory bodies to stay informed on best practices and compliance expectations.

Deadlines:

Effective Date: January 1, 2024

Compliance Requirement for Existing Companies: By January 1, 2025

Ongoing Reporting: Within 30 days of formation or changes to ownership

Industries Impacted:

Financial Services

Fintech & Neobanks

Legal & Corporate Services

Any business forming or maintaining legal entities in the U.S.

Regulator:

Financial Crimes Enforcement Network (FinCEN)

Under the U.S. Department of the Treasury

5. U.S. FinCEN Beneficial Ownership Rule:

Top 3 Impacts for Businesses & Customers:

- 1. Mandatory beneficial ownership reporting:** Companies must submit detailed information on individuals who own or control 25%+ of an entity or exercise substantial control.
- 2. Increased transparency & regulatory scrutiny:** Enhances visibility into shell companies and anonymous ownership, impacting corporate structuring, M&A, and KYC checks.
- 3. Legal & operational risk:** Non-compliance may result in civil and criminal penalties, including fines and imprisonment for willful violations.

Key Actions: Immediate Next Steps for Compliance:

Review entity structures:

Identify all beneficial owners across newly created and existing legal entities.

Update KYC & UBO collection processes:

Integrate beneficial ownership checks into onboarding workflows using tools like the IDnow Trust Platform to automate UBO screening, risk scoring, and document capture.

Prepare for ongoing reporting & audit trails:

Ensure your systems can track ownership changes and trigger timely updates to FinCEN. Leverage platforms that offer full audit trails, timestamped identity checks, and compliance-ready documentation.

6. APAC's KYC & AML Shift

Key dates:

Ongoing regulatory rollout across key markets, with stricter enforcement in 2024–2026

Industries Impacted:

Financial Services

Crypto & Virtual Asset Service Providers (VASPs)

Remittance & Payments

Gaming & Gambling

Fintech

Regulator:

Singapore: Monetary Authority of Singapore (MAS)

Australia: Australian Transaction Reports and Analysis Centre (AUSTRAC)

China: People's Bank of China (PBoC)

Top 3 impacts for businesses & customers:

- 1. Mandatory digital identity verification:** Singapore now requires digital ID verification (e.g., Singpass) and real-time monitoring for high-risk transactions.
- 2. Expanded AML coverage & consultation:** Australia is reforming its AML/CTF laws to extend to crypto, gaming, and high-risk payment providers, with stricter recordkeeping and risk-based controls.
- 3. Licensing & Anti-Fraud Pressure in China:** Facilitates seamless digital interactions across EU member states, expanding market reach.

Key actions: immediate next steps for compliance:

Localise identity verification flows:

Adapt KYC and onboarding flows to support national digital IDs like Singpass, MyGovID, and Chinese resident ID systems.

Implement real-time fraud & transaction monitoring:

Use orchestration tools like the IDnow Trust Platform to dynamically adjust fraud controls and alert mechanisms in high-risk APAC markets.

Monitor regional regulatory updates:

Engage with local legal and compliance experts to stay ahead of evolving requirements and licensing deadlines in each jurisdiction.

Section 2:

The rising fraud threat in 2025



If digital identity is the key to trust, and compliance is the framework that shapes the lock, then fraud is the force that threatens to pick that lock.

In 2025, fraud isn't just evolving – its proliferating at speed. AI-powered attacks, synthetic identities and hyper-personalized social engineering scams are pushing traditional fraud defences to the breaking point. Fraudsters are more sophisticated, scalable, and faster than ever before – leveraging the same technologies that power digital transformation to launch increasingly complex attacks.

Where once it was enough to detect forged documents or mismatched biometrics, today's threat landscape spans far beyond the checkboxes of KYC. We're seeing a sharp rise in deepfake technology used to spoof biometric systems, document tampering that can bypass document verification tools, and synthetic identities that are painstakingly built to mimic real humans across multiple data sources.

But the danger doesn't stop at onboarding. Fraud is now a continuous threat – surfacing at any point in the customer journey. Social engineering attacks, like phishing and vishing, are being amplified by generative AI, making them harder to detect and easier to scale. Fraudsters no longer need to break through security systems – they just need to trick a human.

This isn't just a problem for compliance, risk or IT teams. It's a business risk, a trust risk, and a reputational time bomb. The challenge? Building fraud defences that move as fast as the fraudsters.

The opportunity? Embracing real-time fraud prevention, adaptive biometrics, and AI-driven risk signals that don't just detect fraud – they predict it. The businesses that succeed in 2025 will be the ones that treat fraud not as a one-off checkpoint, but as an ongoing, intelligence-driven process that adapts to every interaction.

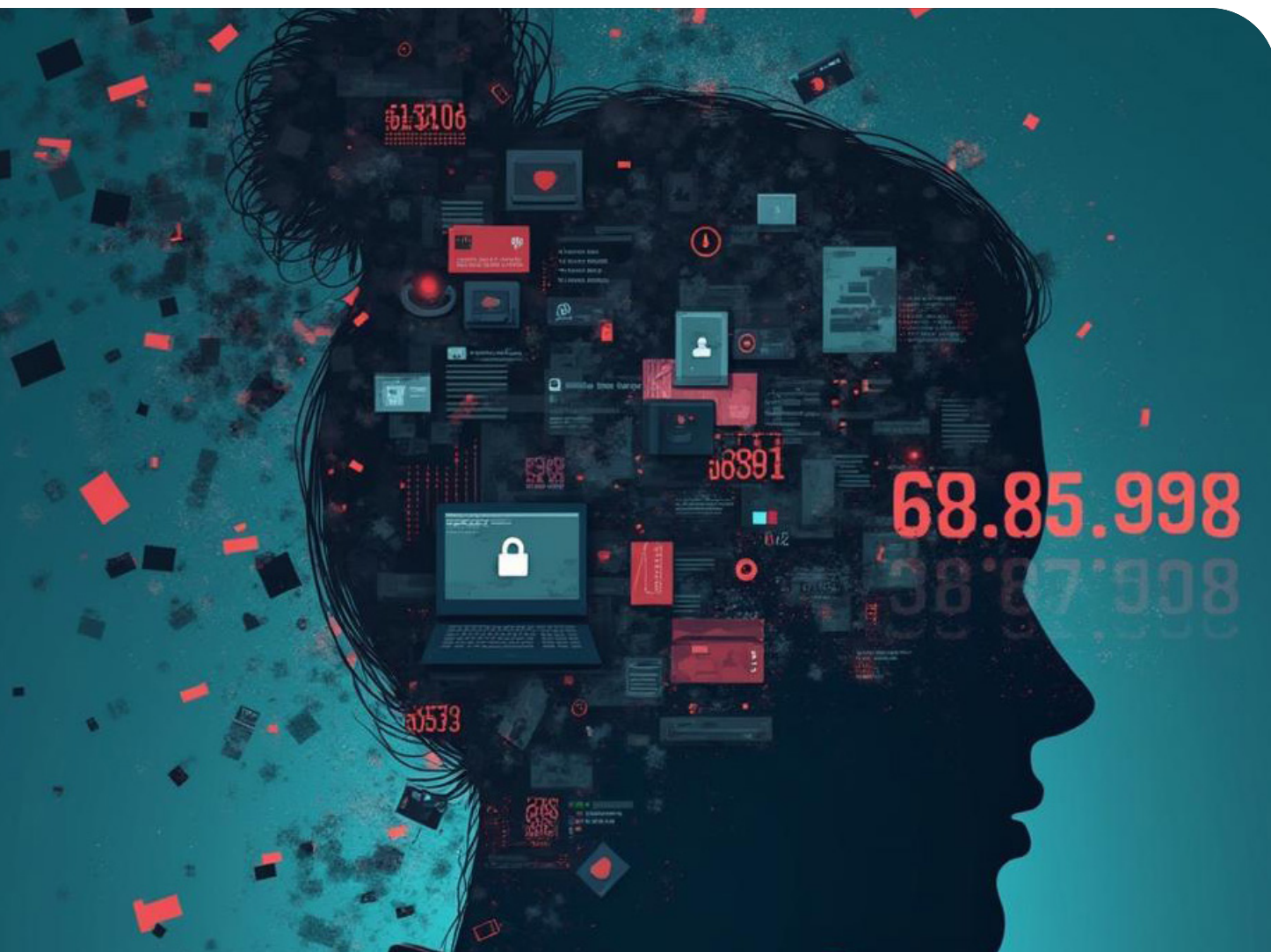
Let's explore the tactics fraudsters are using – and what you need to do to stay ahead.

Identity fraud: stolen data, forged docs, and the price of a name

Every time a data breach hits the headlines, millions of personal details flood the dark web — names, birthdays, ID numbers, addresses, and more. That information becomes the currency of identity fraud: the act of impersonating someone else to open accounts, steal money, or gain access to services.

It's a silent crime, often unnoticed until it's too late — and it's scaling fast.

Fraudsters are stitching together stolen personal details with forged documents to bypass verification systems. Deep web marketplaces offer everything from high-quality fraudulent passports to full synthetic ID kits. With tools like Photoshop and AI-powered image generators, they can create identities that pass most checks.



Why this matters

For Businesses:

Identity fraud isn't just a consumer problem. It leads to fake account creation, money laundering, bonus abuse, and reputational damage. And in regulated industries, the financial and compliance risk is enormous. Businesses that rely on outdated verification methods — or assume a scanned ID is enough — are sitting ducks.

For Customers:

Victims of identity fraud face months of years of fallout – frozen accounts, denied credit, emotional stress. But more than that, it damages their trust in digital systems. Every breach makes people more reluctant to share their data again.

The Challenges.

Data breaches

The lifeblood of identity fraud: Billions and billions of records are exposed every year. In 2023 alone, over 8 billion records were exposed. Once your details are out there, they can be used again and again.

Hard-to-detect fraudulent documents:

Today's fraudulent documents aren't pixelated PDFs. They are near perfect replicas with accurate fonts, holograms and metadata.

Hard to trace:

Unlike a stolen credit card, a stolen identity can be used to build a long-term fake persona that flies under the radar.

The Opportunities.

Document verification and authenticity checks:

Go beyond surface-level scans and detect signs of tampering, template anomalies, and metadata mismatches.

Biometric verification:

Confirm that the person presenting or submitting the document is real – and match that image with the ID document photo, preventing impersonation.

360 fraud signals:

Track patterns across sessions, users and devices. Detect copycat document templates and repeat instances of the same face, template or data or device and flag in real-time.



The **deepfake** arms race

Picture this: A fraudster generates a perfect clone of someone's face using AI. It blinks, it smiles, it even passes a quick selfie check. Now imagine hundreds of these clones being unleashed across platforms, applying for loans, opening crypto wallets, or tricking onboarding systems at scale. Welcome to the deepfake arms race.

Fraud isn't just evolving – it's replicating. AI-generated attacks like deepfakes and voice clones are outpacing traditional detection tools, targeting biometric and document verification processes that once felt bulletproof.

But the good news? Businesses aren't fighting this war alone. Advanced detection technology is fighting fire with fire – using AI to outsmart AI.

Why this matters

For Businesses:

Trust in biometrics has become non-negotiable. If you rely on facial recognition or video ID checks, you need to ensure they are protected against hyper-realistic spoofs that can slip through outdated systems.

For Customers:

Consumers expect their face or ID to be the most secure way to verify who they are. If that trust breaks, the fallout is immediate – loss of confidence, reputational damage, and higher drop-off rates.

The Challenges.

Hyper-realistic reproductions Deepfake technology is now widely available and incredibly convincing. Static liveness checks or legacy systems are no longer enough to stop deepfake fraud.

Speed & scale:

These attacks don't happen one-by-one. Entire fraud rings are using generative AI to scale attacks in real-time, overwhelming unprepared systems.

Trust erosion:

The more consumers hear about deepfakes slipping through, the more they will question whether biometrics are still safe and can be relied upon.

The Opportunities.

Real-time deepfake detection:

AI-powered liveness and deepfake detection technology uses pattern recognition, micro-movement analysis, and challenge-based authentication to spot even the most sophisticated fakes.

AI fighting AI:

By continuously training models on the latest deepfake methods, you can stay one-step ahead of fraudsters – ensuring security evolves as fast as threats do.

Multi-layered protection:

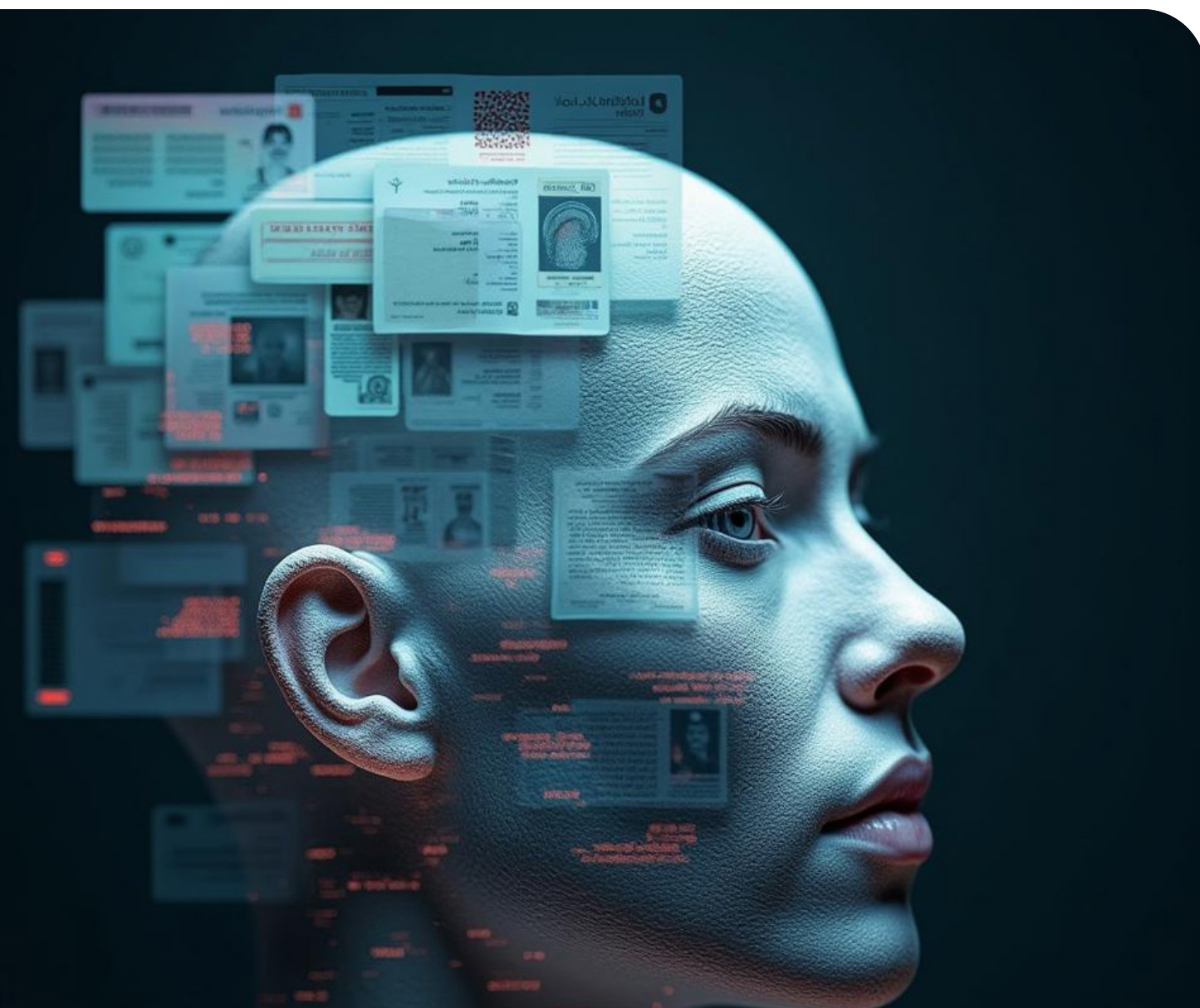
Combining biometric checks with document verification, device intelligence, and behavioural analytics builds a more resilient onboarding process that can't be easily tricked by synthetic media.

Synthetic identities: the fraud you don't see coming

What if the fraudster you just verified doesn't actually exist? They have a valid-looking passport. A working phone number. A face that passes a biometric scan. But behind it all is a meticulously created fake – built from pieces of real and fake data.

That's a synthetic identity, and in 2025, they're not rare – they're rampant. Fraudsters are highly adept at blending real and fraudulent information to create identities that are good enough to pass through standard KYC, create accounts, build credit histories, and commit fraud, weeks – even years – later.

It's not about stealing someone's identity anymore. It's about building a better one.



Why this matters

For Businesses:

Synthetic identity fraud costs billions. Financial institutions are approving accounts for people who simply do not exist – and only discovering fraud after significant damage is done.

For Customers:

These attacks don't just try to game systems – they distort trust in digital onboarding. As more 'ghost' customers slip through the cracks, legitimate users face tighter, slower, and more frustrating verification.

The Challenges.

Blended identities:

Fraudsters use real data – like social security numbers or addresses – and combine this real data with fabricated names, faces and documents. These hybrid identities bypass rigid verification checks designed to catch purely fake profiles.

Undetectable at first glance:

Synthetic profiles often behave like genuine users – making small transactions, updating details, or building trust – until the moment they cash out.

Hard to trace:

Once fraud is discovered, there is usually no real person behind the identity – making recovery and prosecution almost impossible.

The Opportunities.

AI-powered identity recognition:

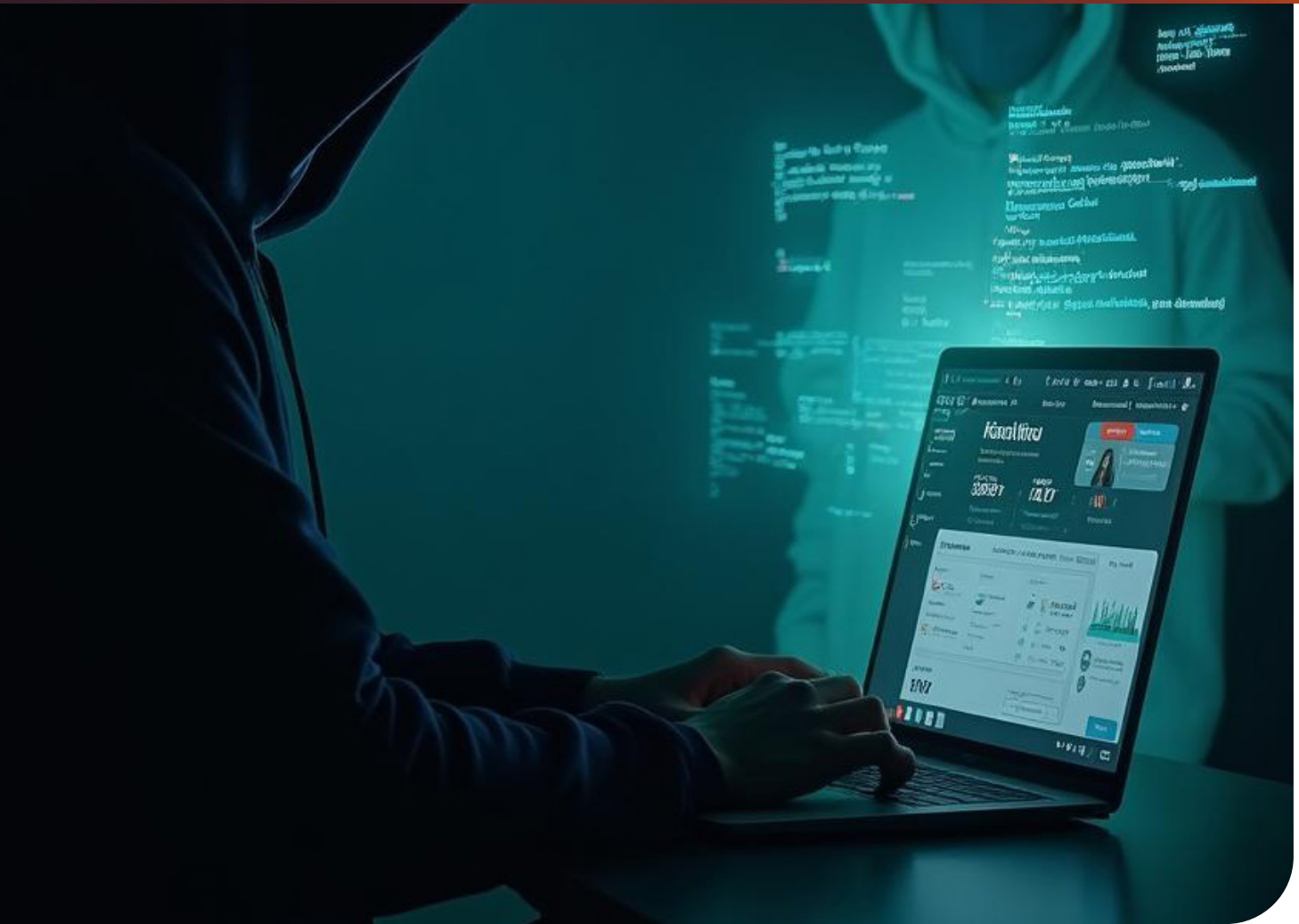
Don't just verify credentials – connects the dots. Holistic risk signals covering everything from the document template to the metadata can identify repeat patterns across data points, documents, and devices.

Template tracking & document intelligence:

Detect if a forged document has been used across multiple onboarding attempts – even if the name, document data and photo change.

Biometric pattern analysis:

Flag when the same face shows up across different submitted identities with advanced facial vector mapping.



Account takeover: when the real user isn't behind the screen

Account takeover (ATO) is one of the fastest-growing types of digital fraud. With data breaches, password leaks, and social engineering on the rise, fraudsters are increasingly gaining access to legitimate user accounts - and using them to steal funds, launder money, or exploit trust.

Why it's so dangerous? Because it doesn't rely on breaking in from the outside - it uses the front door.

ATO attacks are especially problematic in industries like banking, crypto, and ecommerce, where a compromised account can lead to significant financial and reputational damage. And the rise of automated credential stuffing and phishing kits means these attacks can scale fast.

Why this matters

For Businesses:

Traditional authentication methods like passwords or SMS OTPs are no longer enough. When a user logs in, you need to know it's really them - without creating too much friction.

For Customers:

Victims of account takeover can lose money, face blocked accounts, or even get blamed for transactions they didn't make. Rebuilding trust takes time, effort, and can impact customer loyalty.

The Challenges.

Invisible intruders:

Once inside, fraudsters often behave like the legitimate user-making detection hard without additional signals.

Credential leaks are everywhere:

With billions of stolen credentials available on the dark web, password-based security is dangerously outdated.

User friction vs. security:

Adding too many verification steps can frustrate real users and increase churn. The balance is delicate.

The Opportunities.

Step-up authentication with biometrics:

If something looks suspicious - like a login from a new location or high-risk transaction - businesses can trigger a biometric re-verification to confirm the user's identity in real time. Think of it as asking for a selfie instead of a password reset.

Re-identification, not re-registration:

Using biometric step-up and liveness check, companies can re-identify the true account holder in seconds - without forcing them to go through full onboarding again.

Intelligent fraud signals:

Don't just verify once and forget. Constantly analyse behavioral and biometric signals and enable proactive fraud detection. If a face, device, or document has been used suspiciously across other accounts, you should know - and flag it instantly.

App fraud & social engineering: when trust becomes a weapon

Authorised Push Payment (APP) fraud is one of the fastest-growing and most emotionally devastating forms of cybercrime. At its core lies social engineering - a psychological manipulation technique used to trick individuals into giving away sensitive information or willingly transferring money. Fraudsters don't hack systems - they hack people.

They impersonate trusted entities like banks, family members, tech support, or even romantic interests. They create urgency, fear, or false authority to pressure victims into bypassing their own judgment. The end goal? Get the victim to authorise a payment themselves - making it far harder to flag or reverse.

APP fraud is surging in sectors from banking to crypto to online marketplaces. And as scams become more convincing, customers are increasingly falling victim.



Why this matters

For Businesses:

Even though the victim authorised the payment, businesses still face the blame - leading to brand damage, reimbursement costs, and increased regulatory oversight - like in the UK, where new regulations from the Payment Systems Regulator (PSR) now require banks to reimburse APP fraud victims, shifting the financial burden away from consumers and onto financial institutions. This raises the stakes dramatically - making effective prevention not just a reputational issue, but a legal and financial necessity.

For Customers:

Victims often feel ashamed or embarrassed, which delays reporting. By the time they do, the money is gone.

The Challenges.

Emotion over logic:

Social engineering works because it bypasses rational decision-making - exploiting human trust, fear, and urgency.

Invisible to traditional defences:

Because users authorise the transaction themselves, traditional fraud detection tools often miss it entirely.

Tighter regulations ahead:

Countries like the UK are enforcing mandatory reimbursement for APP fraud victims, increasing the pressure on businesses to prevent it upfront.

The Opportunities.

Video Verification as Human Defense

Triggered during high-risk actions - like new payees or large withdrawals - video verification brings trained analysts into the loop. They detect hesitation or coercion in real time, giving businesses a chance to intervene before money is lost.

Smart Fraud Signals

Track red flags like device changes, fast sessions, or odd IPs. Escalate instantly with video checks, biometric re-auth, or transaction blocks.

Beyond the Screen

APP fraud is psychological. Layered systems combining behavior analytics and human judgment can detect when users are being manipulated.



Internal threats: when trust breaks from the inside

Not all fraud comes from the outside. Sometimes the call is coming from inside the house.

From rogue employees stealing data to innocent staff clicking on a phishing link that installs malware or ransomware – internal threats are an often-overlooked part of the fraud equation. Furthermore, we live in the age of hybrid working, BYOD policies and cloud-based systems – so the attack surface is wider than ever and only continuing to expand.

It only takes one compromised device, one weak password, or one disgruntled employee to open the door to devastating breaches and fraud risks.

Why this matters

For Businesses:

Internal fraud can be especially hard to detect – and even harder to prevent. Insiders already have access to systems and data, and when they go rogue (intentionally or by accident), it can cost millions. Malware infections, credential theft, and unauthorized data exports can all be traced back to human error or insider intent.

For Customers:

Consumers assume that when they hand over their data, it's protected. If that trust is broken – especially by an employee on the inside – it can destroy confidence in the brand, even if the consumer is not directly affected.

The Challenges.

Phishing, malware & ransomware: Employees are still the #1 target – they are the weakest link. Sophisticated emails can trick even trained staff into clicking malicious links, installing malware that quietly harvest login credentials and access rights, or in the case of ransomware, preventing access by encrypting devices and data and demanding sums of money for decryption.

Privileged access abuse:

Employees with access to sensitive data – like finance and HR – can become high-risk vectors if not properly monitored or offboarded.

No visibility:

Many businesses lack the tools to detect when insiders are exfiltrating data, misusing systems, or operating under coercion.

The Opportunities.

Step-up authentication:

Verify the identity of users before granting access to sensitive data or systems.

Biometric checkpoints:

Re-identify users at critical moments, ensuring that the person behind the login is who they really say they are.

“Building trust externally starts with securing trust internally. Your employees are your front line – and sometimes, your last line of defense.”

Armin Berghaus,
Chief Technology Officer and
Security Officer, IDnow

Fighting fraud with trust:

Why IDnow is your ultimate defense



Fraud is no longer a one-off threat – it is persistent, intelligent, and an evolving adversary. Whether its deepfakes mimicking real users, synthetic identities flying under the radar, or malware quietly hijacking employee access, the modern fraud landscape is dynamic and dangerous. It blurs the lines between identity, intent, and intrusion – and its only growing in speed and scale.

But the truth of the matter is, fraud doesn't have to be the cost of doing business. With the right strategy, tools and technology, it can be contained, controlled, and ultimately, outsmarted.

That's where IDnow comes in.

At IDnow we believe that trust is not just something you defend – it's something you build and enrich, in real-time, at every interaction.

Our solutions are engineered to make that possible, empowering businesses to stop fraud before it starts, reduce operational losses, and deliver seamless, secure user experiences that customers actually trust.

Here's how we help you take control:

Stop fraud in **real-time** – before it costs you



AI-powered document & biometric verification: IDnow offers the most comprehensive portfolio of identity verification solutions on the market - engineered to help you stay one step ahead of fraud while scaling verification workflows in line with your risk appetite. Whether you require seamless data checks, eID onboarding, fully automated identity verification, manual reviews, or high-assurance video verification, our modular approach lets you flex between speed and security based on your specific business needs.

When it comes to verifying documents, our advanced AI-driven engine performs an extensive range of authenticity checks, from OCR and MRZ validation, to cross-checks against issuing authority data. We go beyond the basics with in-depth analysis of security features like holograms, watermarks and document integrity patterns - ensuring forged and tampered documents are reliably detected. Our document coverage confidentiality captures and verifies over 3,700 documents from more than 215 issuing authorities worldwide.

At the biometric level, our passive liveness technology provides a frictionless yet highly secure user experience - detecting deepfakes, 3D masks and replay attacks without requiring users to perform intrusive gestures or movements. Our biometric engine combines AI-powered facial matching with multiple liveness signals to deliver fast, accurate results with minimal false positives or negatives.



360 signal intelligence: Fraud doesn't happen in isolation - and neither should your fraud detection strategy. Our solutions continuously cross-references data across the identity verification lifecycle to spot patterns and prevent repeat attacks. Whether it's the same biometric template, reused identity information, duplicate documents, or recurring device fingerprints, our AI engine connects the dots in real time. We can detect synthetic identities and coordinated fraud rings by identifying suspicious reuse of faces, templates, devices, and data - even when the individual signals appear legitimate. This intelligence is updated constantly, helping you stop identity theft before it happens and reduce downstream fraud.



Fraud risk intelligence: IDnow enriches every transaction with layered risk signals that go beyond identity checks. From email age and domain analysis to IP reputation, geolocation mismatches, behavioural anomalies, and device trust signals, we uncover hidden threats that typical KYC processes miss. Combined with real-time transaction monitoring and configurable risk thresholds, our system flags suspicious behaviour early - giving you the confidence to block high-risk users and fast-track genuine ones. With fraud detection woven into every step of the journey, you gain a holistic view of trust, risk, and intent - powered by dynamic intelligence that evolves with every interaction.

Balance fraud with friction for seamless UX



Friction when it matters, speed when it counts: At IDnow, we believe that great security shouldn't come at the expense of a great user experience. That's why our identity verification platform is designed to adapt in real time, applying just the right amount of friction based on the context and risk level of each interaction. Low-risk users are fast-tracked through seamless, fully automated flows, while higher-risk cases are intelligently escalated to more robust checks - such as video verification or manual review. This dynamic orchestration ensures maximum security without compromising conversion, helping you deliver smooth, compliant, and scalable journeys from the very first touchpoint.



Trust built across the customer lifecycle: IDnow powers secure identity flows across the entire customer lifecycle - not just at onboarding, but wherever trust needs to be established or re-established. Whether you're authenticating a returning user, managing account recovery, or securing sensitive transactions, our platform flexes to your specific business logic, compliance requirements, and user experience goals. From web to mobile apps to digital wallets, we provide consistent, secure, and user-friendly verification across channels - helping you create a unified experience that feels effortless for your customers and robust for your risk teams.



Zero-trust built for trust: In a world where trust can't be assumed, IDnow brings continuous authentication into every step of the user journey. Our platform doesn't just verify identities once and move on - it actively reassesses trust signals over time, allowing you to spot anomalies, enforce step-up verification, and stop account takeover in its tracks. And we do it without disrupting the user experience, thanks to behind-the-scenes checks that keep users moving unless risk truly demands intervention. It's zero-trust, implemented in a way that protects your users - without ever slowing them down.

The bottom line

Fraud is evolving. But so are we.

IDnow gives you the visibility, agility, and intelligence to turn fraud prevention into a competitive advantage - protecting your revenue, your reputation, and the trust your customers place in you.

Because in 2025, real-time trust is the most valuable currency your business can hold. And we're here to help you protect it.

Section 3:

The technology disruption in digital identity

Why businesses must **stay curious**, not just compliant

What if your biggest risk in 2025 isn't non-compliance, but being left behind by innovation?

As regulations evolve, so too does the technology powering digital identity. AI is rewriting how we detect fraud. Digital wallets are reshaping how we onboard users. And decentralised identity is challenging everything we know about trust online.

The problem? Technology is moving faster than regulation can keep up. That means businesses can't afford to sit back and wait for official guidance. They need to be proactive; experimenting, learning, and adapting now, so they don't find themselves outpaced tomorrow.

Let's explore the three biggest tech trends disrupting identity verification today, and what they mean for businesses who want to stay ahead of the curve.



1. AI & Machine Learning in Identity Verification

Supercharging fraud prevention, but not without risks

Think of AI as your secret weapon against sophisticated fraud. Trained on millions of data points, AI models can detect anomalies humans might miss, like subtle document forgeries or behavioural red flags that signal synthetic identities. It's faster, smarter, and scalable.

But here's the twist: with great power comes great responsibility. AI models can inadvertently introduce bias, exclude vulnerable users, or make decisions that are hard to explain to regulators. That's why AI in IDV is coming under increasing regulatory scrutiny, with upcoming EU AI laws requiring more transparency and accountability from vendors and businesses alike.



What businesses need to think about:

- How explainable is your AI decisioning?
- Can your team audit it and prove fairness and accuracy?
- Are you combining automation with human oversight where needed?

At IDnow, we believe in augmented identity verification. AI where it makes sense, human experts where it matters most. That's why our platform offers flexible workflows that combine both. You get automation where it speeds things up, and human judgment where it adds trust.

2. Digital **Wallets** & Verified Electronic Attributes

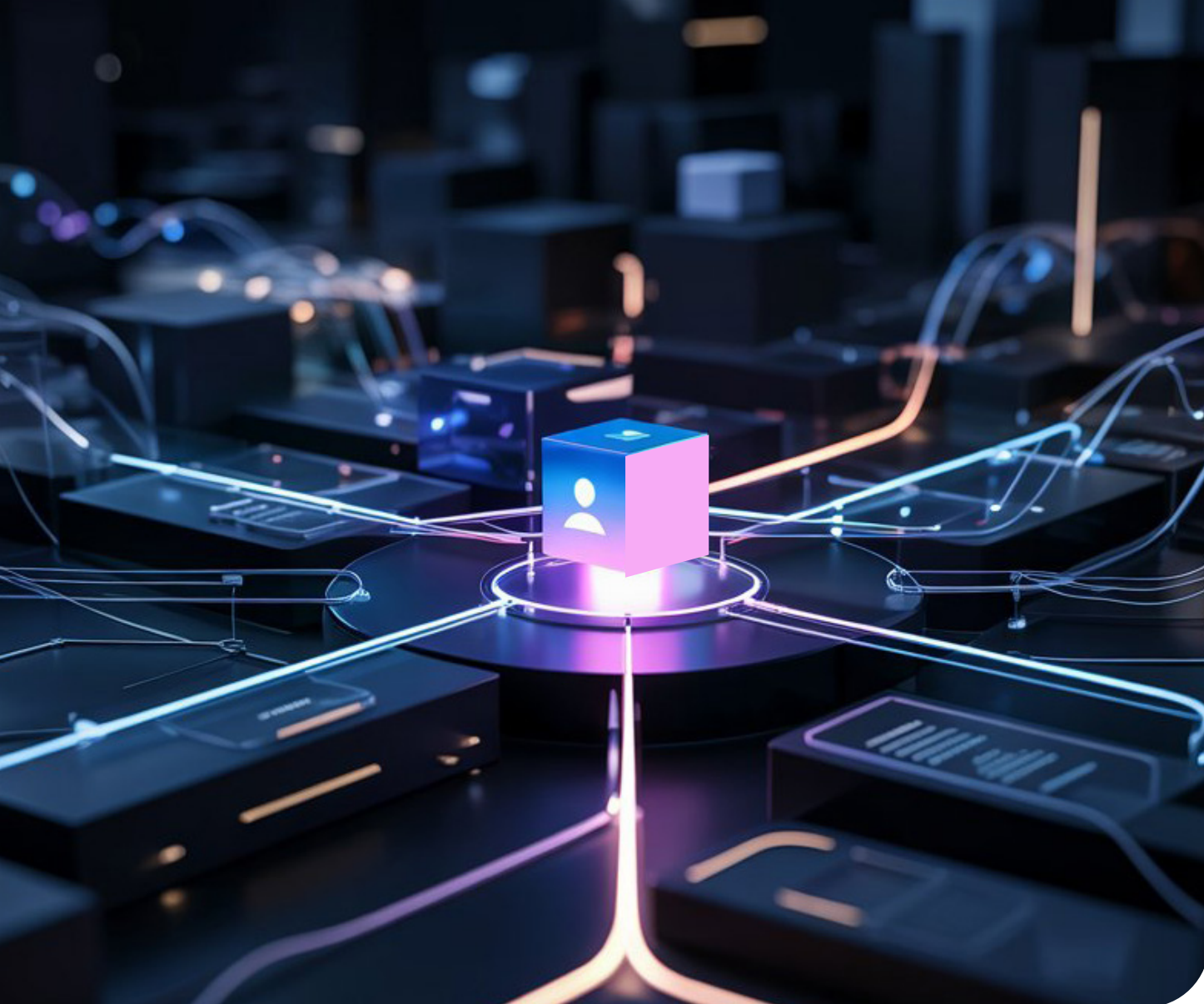
A more private, user-centric model, powered by (Q)EAAs and pub-EAAs

With the EU Digital Identity Wallet and the new trust services under eIDAS2, users will be able to control and share only the identity attributes they need, instantly and securely. From name and age to bank account details, Qualified Electronic Attestations of Attributes (QEAs) and Public Electronic Attestations of Attributes (pub-EAAs) offer a flexible, privacy-preserving way to verify identity without oversharing. The EU is standardising formal attribute-based trust services, issued and verified by qualified entities under strict legal and technical controls.

Sounds ideal, right? But here's the catch:

- Verifying wallet credentials requires new infrastructure.
- Security risks like wallet hijacking, spoofed attestations, and phishing are still emerging.
- And user experience can be clunky, especially when wallets are managed across borders or apps.

That's where orchestration platforms like our Identity & Trust Platform come in.



IDnow.

How the Identity & Trust Platform supports the new attribute-based identity model:

- Accepts and verifies credentials issued in EUDI Wallets, including (Q)EAAs and pub-EAAs via a single API.
- Connects to national wallets across Europe through a harmonised integration layer.
- Combines wallet-based ID with ongoing fraud checks, AML screening, and biometric proofing so you don't just trust the credential, you verify the user.

Think of it as your integration layer between the new world of verified electronic attributes and your existing compliance workflows. We future-proof your identity infrastructure without making you start from scratch.

3. Large Language Models & Generative AI

Boosting efficiency, but creating new fraud frontiers

You've probably already used a large language model (LLM) like ChatGPT to write an email or summarise a report. But did you know these models are also revolutionising identity verification on both sides of the trust equation?

On the positive side, LLMs can supercharge operational efficiency. They're helping teams template communications, classify documents, and triage suspicious patterns faster than ever. They're also being used to enhance user support and streamline internal decision-making.

But more importantly, they're transforming how we respond to fraud.

At IDnow, we've harnessed LLMs to dramatically accelerate how we onboard new identity document templates. In the past, building accurate recognition models for new passports, ID cards or driving licences required collecting and analysing a large volume of physical document samples.



Now, with LLM-assisted learning, we can confidently develop and roll out new document templates with far fewer samples, without compromising on security. This means we can:

- Spot fraud patterns faster
- Stay ahead of emerging document types
- And protect your business from forged IDs long before they become widespread

But while we're using LLMs to strengthen our defences, fraudsters are doing the same.

On the dark side, LLMs are being exploited to:

- Generate fake documents with startling realism
- Script social engineering attacks that sound eerily human
- Bypass verification flows by mimicking user behaviour or language

The IDnow logo is a circular emblem with a thin orange border. Inside the circle, the word "IDnow." is written in a bold, sans-serif font. The "ID" is black, and "now." is orange, matching the border color.

How IDnow is responding:

- We're integrating LLM-powered fraud detection tools into the Identity & Trust Platform
- We cross-check document data with active and historical fraud signals
- We issue real-time alerts on suspicious behaviour, whether at onboarding or during later account activity
- And we're using LLMs to intelligently adapt to new document types and fraud vectors, at speed

Generative AI isn't just a threat, it's also an opportunity. When used responsibly, it becomes a vital part of a smarter, faster, more agile identity verification strategy.

- **Large Language Models (LLMs) & Generative AI**
- LLMs are revolutionising identity on both sides of the trust line.
- **How IDnow uses LLMs to:**
 - Build new document templates faster, with no massive sample sets required
 - Spot and stop fraudulent document types before they spread
 - Accelerate how we respond to new fraud patterns

- **What fraudsters do with LLMs:**
 - Generate fake documents
 - Mimic real users
 - Script deepfake-ready attacks



With the IDnow Trust Platform, we're integrating LLM-powered fraud detection and real-time pattern recognition, so your defences evolve in sync with the threat landscape.

Key takeaway

If your tech stack can't keep up, it's not just outdated, it's dangerous.

The identity world is transforming fast. Build with tech that evolves, with AI, wallets, and fraud detection built-in.



The **essential tech guide**: your future-ready identity stack in 2025

What every tech-savvy compliance and identity leader should be asking now.

AI & Machine Learning

Your fastest route to smarter, scalable fraud prevention

AI doesn't sleep. It detects forgeries, flags anomalies, and helps you fight synthetic identities with speed and scale. But with the EU AI Act around the corner, you need more than just smart models, you need explainable ones.

Checklist:

- ☐ Can your AI decisions be audited and explained?
- ☐ Are you balancing automation with human oversight?
- ☐ Are you training your models on your risks?

IDnow.

At IDnow, we combine automated solutions incorporating machine learning with expert review to deliver augmented/hybrid verification, so you get speed, accuracy, and trust.

Digital Wallets & Decentralised Identity

The EU Digital Identity Wallet is coming fast. Decentralised identity promises privacy, portability, and fewer data silos.

Checklist:

- ☐ Can you verify wallet-based credentials across borders?
- ☐ Is your infrastructure compatible with DID protocols / EUDI Wallet protocols in the ARF?
- ☐ How do you combine wallet trust with ongoing checks?

IDnow.

The IDnow Trust Platform makes wallet integration simple: plug into national and EU wallets, verify credentials, and layer in fraud and AML checks.

Section 4:

Why IDnow is redefining trust



As digital identity landscapes continue to evolve, trust has become the cornerstone of all online interactions, transactions, and relationships. IDnow is leading the way in transforming how businesses approach trust in identity verification. We are evolving from a European provider of automated identity verification solutions into a global leader in digital identity trust, redefining the standards for fraud prevention, compliance automation, and real-time identity management.

The next evolution of identity verification

In today's hyper-connected, digital-first world, trust is no longer a luxury, it's a necessity. Digital identities are fragmented, increasingly under threat, and evolving in complexity. Businesses must create secure, scalable ecosystems of trust that can adapt to these challenges.

IDnow's Trust Platform for trust and fraud prevention

IDnow's Trust Platform is at the forefront of this shift, providing an AI-driven, SaaS-based Identity & Trust Platform for fraud orchestration and compliance automation. This next-generation identity solution ensures businesses can confidently verify identities and prevent fraud across all interactions. Whether it's verifying someone's identity at the point of entry or continuously monitoring trust across the entire customer journey, IDnow is redefining what it means to build a trusted, secure environment.

AI-Driven fraud orchestration & compliance automation

Our platform integrates cutting-edge AI to detect emerging fraud risks in realtime, automate compliance checks, and adapt to evolving regulatory frameworks. Fraud detection is no longer limited to a one-time check, it is now a continuous process that evolves with new threats, helping businesses stay ahead of risks and maintain a secure environment for their customers. This intelligent, adaptive approach ensures businesses can meet current demands and anticipate future challenges.

A global approach to identity

The complexity of managing identity verification and fraud prevention increases as businesses expand globally. Fragmented identity systems and regional regulatory requirements can make it difficult for businesses to provide consistent, secure customer experiences worldwide.

Sorting the chaos of fragmented identity systems

IDnow simplifies this complexity by offering seamless access to digital identities (eIDs), digital wallets, Trust Services, and verification solutions, all powered by real-time risk intelligence. We help businesses sort through the chaos of fragmented identity systems and integrate all necessary elements into a single, scalable solution. This holistic approach enables businesses to focus on growth, while we handle the intricacies of identity verification and fraud prevention.

Helping businesses navigate global regulations

With the rise of regulations like AMLD6, PSD3, and eIDAS2, businesses face increasing pressure to stay compliant across multiple jurisdictions. IDnow is uniquely positioned to help businesses navigate this complexity by providing solutions that meet regulatory requirements and protect against emerging fraud risks. Our Identity & Trust Platform adapts seamlessly to regulatory changes, ensuring that businesses remain compliant and secure no matter where they operate.



At IDnow, we understand that trust is the foundation for every successful business strategy, every seamless transaction, and every lasting customer relationship. Our mission and vision reflect this commitment.



Vision:

Our vision is to be the gateway to a secure digital trust ecosystem where identity isn't just verified but continuously enriched and secured – setting a new standard of trust that drives lasting competitive advantage in the global digital economy.



Mission:

We are IDnow – where trust powers identity. We transform trust into the most powerful asset in the digital world, empowering enterprises with AI-driven, SaaS-based identity solutions that deliver scalable security, adaptive compliance and real-time fraud prevention.



Conclusion:

**Turning compliance chaos
into your competitive
advantage**

In this playbook, we've explored the sweeping changes reshaping the digital identity landscape; from the arrival of eIDAS2 and the EU Digital Identity Wallet, to the tightening grip of AMLR, PSD3, and global fraud regulations. Together, they mark 2025 as a turning point for businesses navigating trust, security, and compliance.

At first glance, it might seem like a regulatory minefield. But look closer, and you'll see a moment of massive opportunity to create smarter customer experiences, streamline operations, and drive secure, scalable growth across borders.

Seizing this opportunity, however, takes more than just ticking boxes. It demands a new mindset where trust becomes a core business driver, built into your digital DNA from day one.

IDnow.

- That's exactly where our **Identity & Trust Platform** can help you. With one **single integration**, we give you:
- Access to all 27 EU Digital Identity Wallets
- Prompt driven workflows tailored to your compliance and UX needs
- Audit-ready documentation to satisfy even the toughest regulators
- 360° fraud prevention, from synthetic identity detection to social engineering and internal threat protection

Ready to turn the insights from this playbook into action?

- ☐ **Get early access updates** on the IDnow Trust Platform
- ☐ Talk to our **product experts about your** identity strategy

Let's **transform** compliance into confidence,
and **trust** into your greatest competitive
advantage.



IDnow is a leader in digital identity and fraud prevention in Europe with a mission to transform trust into the most powerful asset in the digital world. Through its broad portfolio of digital identity and fraud prevention solutions, IDnow establishes, maintains and enriches trust throughout the customer journey, ensuring businesses can confidently and securely operate while leveraging digital identity to drive growth, security and scalability.

IDnow completes more than 7.5m KYC checks per month, supports more than 3,700 documents globally from 215 issuing authorities and covers documents from 157 countries.

The company has offices in Germany, United Kingdom, and France and its portfolio of international clients spans a wide range of industries.

www.idnow.io