

## PSD3 & PSR READINESS:

Building an Intelligence-Led Approach to Fraud Prevention, Payment Trust and Regulatory Readiness

---

More than a regulatory update, PSD3 and PSR signal a new era of fraud accountability across the EU payments ecosystem.



PSD3

Payment



PSR

## A new era of fraud accountability

The combination of instant payments, sophisticated scams, evolving liability expectations and growing consumer protection requirements is reshaping how organizations need to manage fraud risk. Payment Services Directive 3 (PSD3) and the Payment Services Regulation (PSR) reflect this shift, placing greater emphasis on real-time prevention, accountability and proactive intervention.

This ebook helps you gain a deeper understanding of PSD3 and PSR, the challenges they introduce and the capabilities organizations need to strengthen fraud prevention, reduce risk and prepare with confidence.

# Contents

|                                                          |    |
|----------------------------------------------------------|----|
| <b>PART ONE: Understanding the Regulatory Shift</b>      | 4  |
| The Forces Reshaping Fraud Prevention                    | 5  |
| PSD3 & PSR: What's Changing and Why                      | 6  |
| What it Means for Today's Organizations                  | 8  |
| <b>PART TWO: Practical Framework for PSD3 Readiness</b>  | 15 |
| The Five Pillars of PSD3 Readiness                       | 16 |
| Building a Future-Ready, Intelligence-Led Fraud Strategy | 22 |
| Next Steps for Getting Started                           | 25 |



# PART ONE: Understanding the Regulatory Shift

# The forces **reshaping** fraud prevention

Rising scams, faster payments, AI-enabled fraud and increasing consumer protection expectations are reshaping how organizations manage fraud risk.

## Scams Are Becoming More Sophisticated



Fraudsters are increasingly exploiting social engineering, impersonation scams and AI-generated deception to manipulate legitimate users into authorizing fraudulent payments. In many cases, criminals pose as trusted organizations such as banks, police or government agencies, creating urgency and convincing victims to move funds under false pretenses.

## Instant Payments Reduce Time to Act



As payment speeds accelerate, organizations have only seconds to assess risk, identify manipulation and intervene before funds move.

€4.2B

payment fraud losses across the European Economic Area

More than 50%

of fraud value associated with credit transfers in the European Economic Area is now linked to payer manipulation and scam-related fraud

## Fraud Is Moving Beyond Traditional Controls



Authentication and account validation alone are no longer enough. Organizations need visibility across customer behavior, device activity and transaction risk to identify fraud earlier.

## Customer Expectations Continue to Rise



Organizations must balance stronger fraud controls with seamless payment experiences while navigating growing expectations around consumer protection, reimbursement and accountability.

As fraud becomes faster, more sophisticated and increasingly AI-enabled, organizations need the ability to identify manipulation, assess risk and make confident decisions before funds move.

This growing need for proactive, intelligence-led fraud prevention is a key driver behind PSD3 and PSR.<sup>1</sup>

# Why is the industry moving beyond PSD2?

The payments landscape evolved faster than the regulatory framework designed to govern it.

PSD2 played a critical role in modernizing European payments by improving security, increasing competition and accelerating Open Banking adoption. However, the payments landscape continued to evolve.

Fraud became more sophisticated, particularly through the rise of authorized push payment (APP) fraud and impersonation scams, where criminals manipulate consumers into authorizing payments themselves. At the same

time, implementation varied across member states, consumer protection expectations increased and the industry began looking beyond Open Banking toward a broader Open Finance future.

**PSD3 and PSR were introduced to address these emerging challenges by creating a more consistent, prevention-led framework that better reflects today's fraud, risk and payments environment.**

PSD3

✓ **Improve** consumer protection

✓ **Enhance** the security of digital payments

✓ **Boost** competition and innovation

✓ **Strengthen** Open Banking and enable Open Finance

PSR

## PSD2 Challenges

Fragmented  
implementation



Harmonized  
framework

Rising fraud



Stronger fraud  
prevention

Inconsistent consumer  
protection



Greater accountability and  
consumer protection

Varying  
enforcement



Consistent enforcement  
across the EU

The goal:

a more secure, innovative  
and consistent payments  
ecosystem that supports  
both consumer trust and  
future growth.

# What are PSD3 and PSR?

## The two regulatory instruments shaping the future of EU

The rise of sophisticated impersonation scams, instant payments and increasing fraud accountability exposed limitations in the PSD2 framework.

In response, the European Union introduced **PSD3 (Payment Services Directive 3)** and the **Payment Services Regulation (PSR)** to create a more consistent, modern framework for digital and electronic payments.

Together, PSD3 and PSR represent a fundamental shift from fragmented compliance and reactive fraud controls toward real-time fraud prevention, stronger consumer protection, reimbursement accountability and greater responsibility for preventing scam-driven payment losses across the payments ecosystem.

### PSD3

Modernizes the regulatory framework for payments

- ✓ Licensing
- ✓ Supervision
- ✓ Governance
- ✓ Open Finance evolution

### PSR

Establishes a single rulebook for how payments operate

- ✓ Payment execution rules
- ✓ Fraud controls
- ✓ Consumer protection
- ✓ Open Banking requirements

+

=

## Future Framework in EU Digital Payments



A more consistent, prevention-led approach to fraud prevention, consumer protection and accountability across the EU.

# How PSD3 is different from PSD2

**PSD3 is best viewed as an evolution of PSD2, rather than a complete replacement.** While PSD2 focused on improving access, authentication and competition through Open Banking, PSD3 and PSR expand the focus to include fraud prevention, consumer protection and operational accountability in a rapidly changing payments landscape.

| PSD2                                                      | PSD3 + PSR                                                                           |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------|
| Enabled Open Banking and digital payment innovation       | Strengthens the foundation for Open Finance and future payments innovation           |
| Focused on authentication and secure access               | Emphasizes prevention, intervention and fraud accountability                         |
| Allowed varying implementation across member states       | Creates a more harmonized EU-wide framework                                          |
| Focused on detecting fraud and protecting credentials     | Focuses on preventing impersonation scams and payment manipulation before funds move |
| Limited emphasis on reimbursement and scam accountability | Greater focus on consumer protection, liability and reimbursement expectations       |
| Account validation and payment security                   | Broader payee verification and transaction risk controls                             |

**Organizations are increasingly expected to identify, assess and intervene before fraud occurs, rather than investigate losses after the fact.**

## Lessons Learned in the UK

The UK's experience with fraud reimbursement requirements highlights the importance of operational readiness, efficient case handling and strong consumer protections as accountability expectations continue to evolve.

88%

**Claims reimbursed**

Totaling £175m – 64%  
prior to regulation

82%

**Claims closed in 5 business days**

Rapid resolution demonstrates  
operational readiness

86%

**Claims reported  
within 2 hours**

From sending to  
receiving bank

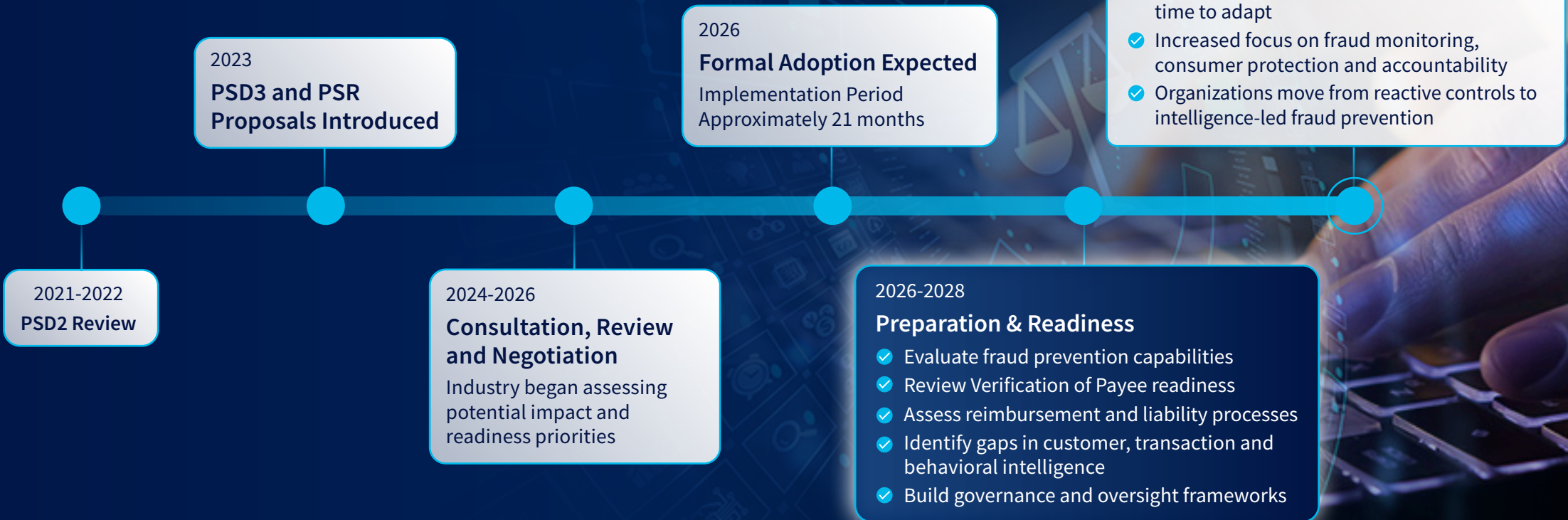
3%

**Rejected for gross  
negligence**

Low rejection rate reflects  
consumer-friendly approach

# Timeline

PSD3 and PSR have progressed through several years of consultation, review and negotiation. While implementation is expected to be phased, organizations should use this transition period to assess gaps, strengthen fraud controls and prepare for a more prevention-led regulatory environment.



## Who is Impacted?

PSD3 and PSR will affect virtually every organization involved in initiating, processing or facilitating payments.

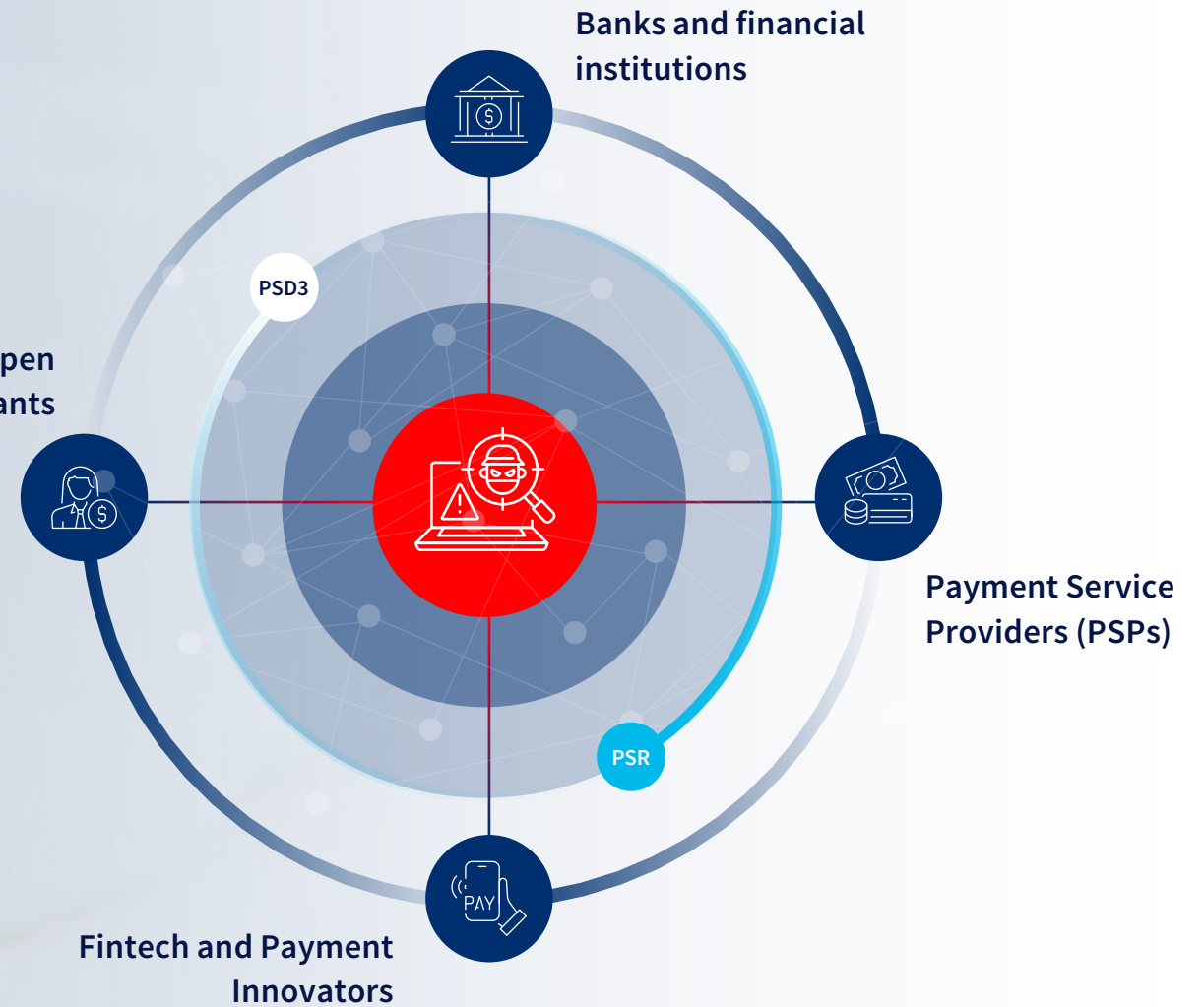
While specific obligations will vary, the reforms extend beyond traditional banks and will impact a broad range of financial services and payment ecosystem participants.

Open Banking & Open Finance Participants

Banks and financial institutions

Payment Service Providers (PSPs)

Fintech and Payment Innovators



# The shift from compliance to fraud prevention

PSD3 and PSR elevate fraud prevention from an operational function to a strategic business priority.

Historically, fraud programs focused on detecting and investigating suspicious activity after it occurred.

Today, organizations are increasingly expected to identify, assess and intervene before fraud occurs and before funds leave an account. At the same time, fraud prevention is moving beyond the responsibility of a single institution.

As scams become more sophisticated and payment ecosystems become more interconnected, organizations need greater visibility across customers, accounts, transactions and counterparties.

PSD3 and PSR encourage a more collaborative approach to identifying, assessing and preventing fraud across the payments ecosystem.

Success increasingly depends on the ability to identify risk, assess intent and intervene before fraud occurs.

What this means in practice:



**Fraud prevention becomes a frontline control**



**Real-time decisioning at scale**



**Liability exposure increases**



**Layered intelligence is now essential**

# Key regulatory changes

A stronger focus on fraud prevention, accountability and consumer protection across the payments ecosystem.

As PSD3 and PSR reshape the regulatory landscape, organizations will need to adapt to a number of significant changes designed to strengthen fraud prevention, improve payment security and create greater consistency across the EU.



## Real-time fraud monitoring

**Assess risk and make confident decisions before funds move.**

Instant payments compress decision windows, requiring organizations to identify and assess fraud risk in real time.



## Verification of Payee (VOP) expansion

**Strengthen payee validation and payment trust.**

VOP expands the role of account and payee verification to help reduce misdirected payments and APP fraud.



## Greater fraud accountability

**Increase readiness for reimbursement and consumer protection obligations.**

As expectations around scam prevention grow, fraud controls, reimbursement processes and customer protection become more closely connected.



## Data sharing and collaboration

**Detect emerging threats through broader intelligence sharing.**

New provisions encourage greater collaboration and insight sharing across the payments ecosystem to identify fraud patterns, mule activity and emerging threats earlier.

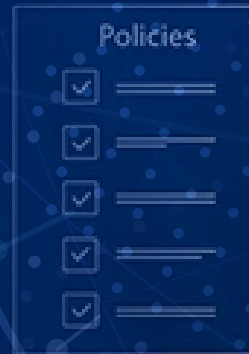


## Security and customer experience

**Strengthen protection without adding unnecessary friction.**

Organizations must balance stronger fraud controls with seamless payment experiences through approaches such as trusted-device recognition, risk-based authentication and intelligence-led decisioning.

# PART TWO: A Practical Framework for PSD3 Readiness



# The five pillars of PSD3 readiness

PSD3 readiness requires capabilities that help organizations make real-time fraud decisions before funds are sent, strengthen payee and transaction intelligence, monitor risk across the full payment lifecycle, detect behavioral indicators of scams and social engineering and leverage network intelligence to identify emerging fraud threats.

Investments in real-time decisioning, risk intelligence, behavioral intelligence and fraud orchestration can help organizations prepare for regulatory change while also reducing losses, improving operational efficiency and creating optimized customer experiences.

Together, these capabilities form the foundation of a more proactive, intelligence-led approach to fraud prevention.

1



✓ Stop fraud before funds move

2



✓ Detect scams and social engineering earlier

3



✓ Monitor trust across the full payment flow

4



✓ Strengthen authentication at onboarding

5



✓ Leverage unified intelligence and orchestration

# 1 Stop fraud before funds move

## Real-Time Fraud Decisioning Starts with Understanding Risk Before Payment Authorization

Organizations have only milliseconds to identify risk before a payment is authorized. Preventing fraud before funds move requires more than transaction monitoring alone.

Effective decisioning depends on combining multiple sources of intelligence to assess risk, intent and trust in real time.

- ✓ API-based decision-making in milliseconds
- ✓ Risk scoring at payment initiation before funds are sent
- ✓ No manual dependencies or delays

Can I trust the transaction?



## INTELLIGENCE-LED RISK ASSESSMENT

- ⚠ Known device by user?
- ⚠ Indicators of compromise, emulation or remote access?
- ⚠ Previous risk association with the digital identity?
- ⚠ Abnormal behavior?
- ⚠ Signs of urgency, coercion or manipulation?
- ⚠ Transaction amount or destination unusual?
- ⚠ Consistent with historical customer payment patterns?



Real-time Decision

## 2 Detect scams and social engineering

### Identify Manipulation Before It Becomes Fraud

Many APP scams originate not from compromised credentials, but from manipulated customers. Investment scams, impersonation scams, romance scams and other forms of social engineering often involve legitimate users authorizing payments under false pretenses.

To identify these threats earlier, organizations need visibility beyond authentication and transaction monitoring alone.

- ✓ Validate identity and account ownership with added fraud context
- ✓ Clearly classify payees as trusted, suspicious or high risk
- ✓ Uncover robust behavioral intelligence for critical context into the event (e.g., social engineering and unusual user-device interactions)
- ✓ Detect unusual activity, payees and transaction patterns
- ✓ Identify high-risk scenarios earlier in the payment journey

Can I trust the user's intent?



Payment Initiated

### INTELLIGENCE-LED RISK ASSESSMENT

- ⚠ Account ownership verified?
- ⚠ Sudden changes in activity?
- ⚠ Deviations from normal payment behavior?
- ⚠ Indicators of social engineering? Abnormal mouse movements or typing patterns?
- ⚠ Active call detection?
- ⚠ Remote access tools?
- ⚠ Newly added payees?
- ⚠ High-risk beneficiary?
- ⚠ Mule network intelligence detected?



Real-time Decision

### 3 Monitor trust across the full payment flow

#### Trust Should Extend Beyond the Sender

As scams, mule activity and beneficiary-related fraud continue to evolve, organizations need visibility across the entire payment flow, from payer to beneficiary. Monitoring trust throughout the payment journey helps identify hidden risk before funds move.

Payment trust should be established across both sides of the transaction. Combining payer, beneficiary, payment and network intelligence helps organizations identify hidden risk earlier, strengthen fraud prevention and make more confident payment decisions.

- ✓ Inbound and outbound transaction monitoring
- ✓ Risk-based alerts and interventions
- ✓ Enable customer warnings at the right moment, based on risk (e.g., before APP scam funds are sent)

Can I trust the recipient?



Payment Initiated

#### INTELLIGENCE-LED RISK ASSESSMENT

- ⚠ Verified payee?
- ⚠ Newly added beneficiary?
- ⚠ High-risk beneficiary patterns?
- ⚠ Aligned to previous activity for the user?
- ⚠ Any signs of scam or mule activity?
- ⚠ Have funds been routed through other high-risk accounts?
- ⚠ Prior fraud activity linked?
- ⚠ Is there an established payment history?



Real-time Decision

## 4 Strengthen authentication at onboarding

### Establish a Trusted Foundation from Day One

Fraud prevention begins long before a payment is made. As synthetic identities, document fraud, deepfakes and account opening fraud become more sophisticated, organizations need greater confidence in who they are onboarding and authenticating throughout the customer lifecycle.

Building trust starts with verifying identity, validating authenticity and continuously assessing risk over time.

- ✓ Build a trusted baseline to reduce downstream fraud risk
- ✓ Leverage market-leading document authentication and facial biometric verification when high-risk transactions occur
- ✓ Continuously validate identity across the customer lifecycle

Can I trust the identity?



Payment Initiated

### INTELLIGENCE-LED RISK ASSESSMENT

- ⚠ Indicators of synthetic or manipulated identity?
- ⚠ Trusted device previously associated with the user?
- ⚠ Confirmed fraud associated previously?
- ⚠ Is a real person behind the interaction?
- ⚠ Does facial biometrics confirm liveness?
- ⚠ ID documents authentic and untampered?
- ⚠ ID documents match the identity?
- ⚠ Indicators of credential compromise or account takeover risk?



Real-time Decision

## 5 Leverage unified intelligence and orchestration across the payment lifecycle

### See beyond your four walls to strengthen decisions

Fraud signals rarely appear in isolation. Customer behavior, identity, devices, beneficiaries and payment activity each provide valuable insight, but the greatest value comes from understanding how those signals relate to one another.

Organizations should focus on unifying intelligence sources and applying them consistently across the payment lifecycle to create a more complete view of risk. This supports more informed decisions, earlier intervention and greater operational efficiency.

- ✓ Automate and scale risk decisions
- ✓ Detect emerging scam risks in real time, based on activity observed across the network
- ✓ Streamline decisioning and reduce manual lift with a single, unified platform
- ✓ Combine identity, device, behavioral and transaction signals through one API
- ✓ Apply risk scoring across the end-to-end payment journey

How do I bring all of these signals together to make better decisions?



### INTELLIGENCE-LED RISK ASSESSMENT

- ✓ Identity intelligence
- ✓ Digital identity and device intelligence
- ✓ Behavioral intelligence
- ✓ Transaction and beneficiary intelligence
- ✓ Network and consortium intelligence



Real-time Decision

- ✓ More accurate decisions
- ✓ Earlier fraud detection
- ✓ Better customer outcomes
- ✓ Faster intervention



## Building a Future-Ready Fraud Strategy

The future of fraud prevention is not built on a single control.

It is built on the ability to combine identity, device, behavioral, payment and network intelligence to identify risk earlier, assess intent more accurately and stop fraud before funds move, bringing together multiple sources of intelligence to create a more complete view of risk across the customer and payment journey.

By connecting these intelligence layers through real-time decisioning, institutions move beyond point solutions to make faster, more confident decisions while balancing security, customer experience and regulatory readiness.

# How LexisNexis® Risk Solutions Can Help

By bringing together trusted intelligence, AI-powered risk decisioning and a unified orchestration platform, we help organizations detect fraud earlier, strengthen trust and accelerate PSD3 and PSR readiness.



## Identity Intelligence

Built on trusted identity data, market-leading document authentication, identity verification and facial biometrics capabilities to establish confidence in who is behind every interaction.



## Digital Identity & Device Intelligence

Powered by industry-leading digital identity and device intelligence, helping organizations recognize trusted users, identify compromised devices and uncover hidden indicators of fraud.



## Behavioral Intelligence

Uncover user intent, even when it's the first interaction with your organization. Analyze behavioral patterns to identify manipulation, social engineering and emerging risks that traditional controls often miss.



## Beneficiary and Transaction Intelligence

Go beyond payment details to gain deeper insight into the risk profiles of both parties involved in a transaction. Leverage beneficiary, account and transaction intelligence to identify high-risk payments, detect mule activity and help stop fraud before funds move.



## Network & Consortium Intelligence

Extend visibility beyond your institution with one of the world's largest cross-industry intelligence networks, analyzing more than 142 billion transactions annually to uncover mule activity, emerging threats and connected fraud patterns.



## Decisioning Layer

Turn intelligence into real-time action through a single decisioning platform. Bring together identity, digital, behavioral, payment and network intelligence to automate decisions, orchestrate workflows and improve fraud outcomes at scale.

## Key takeaways

### ✓ **PSD3 and PSR represent more than a regulatory update.**

They signal a broader shift toward fraud prevention, consumer protection and accountability across the payments ecosystem.

### ✓ **Fraud prevention is becoming an enterprise-wide priority.**

Fraud is no longer confined to fraud operations teams. It increasingly impacts financial performance, customer trust, operational resilience and regulatory readiness.

### ✓ **Real-time decisioning is becoming essential.**

Organizations must identify risk and intervene earlier as payment speeds accelerate and fraud becomes more sophisticated.

### ✓ **Single-point controls are no longer sufficient.**

Authentication, account validation and static rules alone cannot provide the visibility needed to identify modern scams, social engineering and payment manipulation. Organizations increasingly require layered intelligence across identity, behavior, devices, payments and network activity.

### ✓ **Early preparation creates long-term advantage.**

Institutions investing now in fraud capabilities, governance and intelligence-driven decisioning will be better positioned to adapt as expectations continue to evolve.

# Your next steps

## 1 Assess Current Readiness

Evaluate fraud monitoring capabilities, Verification of Payee readiness, liability exposure and existing fraud controls.

## 2 Identify Intelligence Gaps

Assess whether current controls can effectively identify:

- ✓ APP scams and customer manipulation
- ✓ Mule activity
- ✓ Beneficiary risk
- ✓ Emerging fraud patterns
- ✓ Cross-channel risk signals

## 3 Strengthen Governance & Operating Models

Establish clear ownership, reporting structures, metrics and accountability frameworks to support evolving fraud responsibilities.

## 4 Modernize Fraud Detection & Decisioning

Move beyond static controls by incorporating identity, device, behavioral, payment and network intelligence into fraud decisions.

## 5 Build for Continuous Adaptation

PSD3 readiness should be viewed as an ongoing capability-building initiative rather than a one-time compliance exercise. Design programs, processes and technology foundations that can evolve as requirements mature.

PSD3

## Building Trust, Preventing Fraud and Preparing for What's Next

PSR

PSD3 and PSR represent more than the next evolution of payments regulation. They signal a broader shift toward real-time fraud prevention, stronger consumer protection and increased accountability across the payments ecosystem.

As fraud becomes faster, more sophisticated and increasingly interconnected, organizations must move beyond traditional approaches.

Success will depend on the ability to identify risk earlier, make confident decisions in real time and bring together the intelligence needed to stop fraud before funds move.

**The organizations best prepared for PSD3 and PSR will not simply adapt to regulatory change. They will use it as an opportunity to modernize fraud strategies, strengthen customer trust and build a more resilient, intelligence-led foundation for the future of digital payments.**

# Prevent fraud earlier, decide faster and scale efficiently without added friction.

Contact us to learn how we can help you prepare for PSD3 and PSR.

**Sources:**

<sup>1</sup> European Banking Authority (EBA) & European Central Bank (ECB), Joint Report on Payment Fraud, 2025.



## About LexisNexis Risk Solutions

LexisNexis® Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers.

For more information, please visit [www.risk.lexisnexis.com](http://www.risk.lexisnexis.com) and [www.relx.com](http://www.relx.com). Our solutions assist organizations with preventing financial crime, achieving regulatory compliance, mitigating business risk, improving operational efficiencies and enhancing profitability.

This document is for informational purposes only and does not guarantee the functionality or features of any LexisNexis® Risk Solutions products identified. LexisNexis Risk Solutions does not represent nor warrant that this document is complete or error free.

LexisNexis and the Knowledge Burst logo are registered trademarks of RELX Inc., registered in the U.S. or other countries. Other products and services may be trademarks or registered trademarks of their respective companies.

Copyright © 2026 LexisNexis Risk Solutions.