Ten Seconds to Get It Right: From Transaction Screening to Customer Screening

The EU Instant Payments Regulation leaves no room for screening during the payment itself. Compliance teams have had to rethink their entire approach.

KEY TAKEAWAYS

1. The impact of the European Union Instant Payments Regulation has been felt throughout the payments industry.
2. The IPR requires a shift from one-time transaction screening to periodic customer screening.
3. The quality of the underlying client data and sanction datasets is particularly important under this new screening situation.

The EU Instant Payments Regulation (IPR), which entered into force in 2024, requires that euro-denominated credit transfers across the Single Euro Payments Area (SEPA) are settled within 10 seconds. Non-eurozone countries must implement the rule in two phases in 2027. The regulation applies to all euro-denominated transactions, even when involving non-eurozone countries.

The IPR requires a fundamental overhaul of screening practices, so compliance teams have had to rethink their entire approach.

The stakes extend well beyond sanctions screening alone, as Olivier Praneuf, Head of Corporate and PSP Business Development at BNP Paribas, points out:

10 s
Settlement deadline for euro credit transfers across SEPA

Daily
Customer screening against EU sanctions, at least once every calendar day

2027
Two-phase implementation for non-eurozone countries



> **"As instant payments become the standard across Europe, the industry's challenge is no longer simply to move money in less than ten seconds, but to make critical risk and compliance decisions within the same timeframe. Verification of Payee, sanctions screening and fraud prevention must all operate in real time while accommodating increasingly diverse payment ecosystems. For PSPs collecting and paying funds on behalf of their clients, traditional beneficiary verification models may not always reflect the reality of the payment flow, requiring pragmatic and innovative approaches. Yet Verification of Payee alone cannot prevent fraud and must be complemented by other robust, prevention measures. At BNP Paribas, we are continually adapting our payment services, investing in advanced fraud detection capabilities, including AI-based models, and working alongside clients and market participants to ensure that instant payments remain both seamless and secure. Ultimately, trust will be the key enabler of broader instant payment adoption."**

Olivier Praneuf | Head of Corporate and PSP Business Development
BNP Paribas

Periodic Screening of Customer Base

The traditional approach is to receive a payment order and then conduct the full sanctions screening of the sender, receiver, and other data contained in the payment message.

In a pivot away from transaction screening, institutions are now required to screen their customers daily against EU sanctions to verify if a payment service user is subject to targeted financial measures. Many organisations accomplish this by screening against a sanctions or risk database. This daily requirement helps identify potential matches earlier, giving compliance teams more time to resolve alerts, ideally before a payment order is submitted.

According to the IPR text[1], payment service providers shall verify their users "at least once every calendar day", and also "immediately after the entry into force of" new restrictive measures or amendments to such measures. The regulation also states that during the payments themselves, providers shall not run the screenings.

This daily requirement helps identify potential matches earlier, giving compliance teams more time to resolve alerts, ideally before a payment order is submitted.

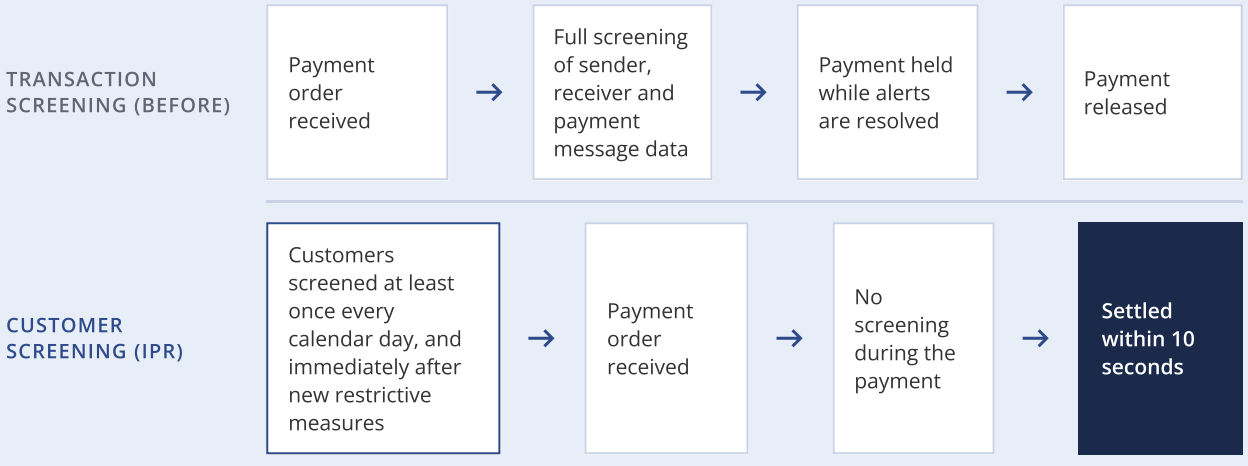
This repositioning of controls is precisely what the regulation is designed to achieve, as Sushil Job, Head of Product Management, European Payments Products at FIS, explains:



"Instant payments require more than making existing controls run faster; they require us to rethink where those controls sit in the payment journey. The regulation itself reflects this approach: Verification of Payee happens before payment authorization, while certain targeted financial sanctions are addressed through daily customer screening rather than additional screening during payment execution. The harder challenge is the exceptions that cannot be resolved automatically and require further investigation within very tight payment timelines. Better data, greater automation and risk-based decisioning can help make those exceptions rarer, allowing speed and effective financial-crime controls to coexist."

Sushil Job | Head of Product Management, European Payments Products
FIS

From transaction screening to customer screening



1. Regulation (EU) 2024/886 of the European Parliament and of the Council, eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202400886

Underlying Data

The quality of the outcome of customer screening will depend largely on the quality of both the organisation's internal data and the external sanctions screening datasets.

The increasing complexity of sanctions regimes has made the external data more challenging to manage. This includes the accurate spelling of names and places, correct dates, personal relationships and complex, evolving corporate structures that may be used to obfuscate sanctions-related ownership or control. Screening against an outdated sanctions database undermines the validity of the checks. At the same time, identifying and maintaining a comprehensive, up-to-date database for verification presents its own challenges.

A sanctions database must be updated constantly; otherwise continuous screening cannot deliver meaningful and timely results. Independent verification is paramount. Screening should draw on reliable intelligence beyond officially published lists, where appropriate. Information must be precise enough to minimise false alerts.
Once a case is escalated for manual resolution, the information must also be structured to support rapid and precise analysis.

WHAT GOOD DATA LOOKS LIKE

- **Updated constantly** — otherwise continuous screening cannot deliver meaningful and timely results
- **Independently verified** — drawing on reliable intelligence beyond officially published lists, where appropriate
- **Precise** — enough to minimise false alerts
- **Structured** — to support rapid and precise analysis once a case is escalated

Some institutions have drawn the architectural consequences of this. Patrick Green, Chief Compliance Officer at Banking Circle, describes the approach taken there:



"We've embedded compliance checks directly into the payment infrastructure, rather than bolting them onto settlement as a separate step. A key part of that is data: moving toward structured, trusted data sources rather than manual, document-based checks that can't keep pace with a ten-second window. Regulation like the EU's AMLR gives us a mandate to make that shift, replacing jurisdiction-by-jurisdiction reconciliation with a clearer common standard to build toward."

Patrick Green | Chief Compliance Officer
Banking Circle

With anticipatory screening conducted before a transaction order is received, the likelihood that transactions will need to be held for screening is significantly reduced. The remaining bottleneck, manual resolution, depends heavily on the data quality across these dimensions. High-quality data is therefore essential to delivering the speed and accuracy required, reducing residual risk, and correctly classifying a potential match as a false positive.

Manual resolution of sanctions screening alerts is where the race against time and the importance of data quality become most apparent. The better the information is presented – structured, timely, detailed and above all accurate – the faster and more reliably escalated cases can be resolved. This is essential both to prevent transactions involving sanctioned parties from being executed and to ensure that legitimate transactions are processed without unnecessary delay.

The better the information is presented – structured, timely, detailed and above all accurate – the faster and more reliably escalated cases can be resolved.

Getting there, however, is not something compliance teams can achieve on their own. As Patrick Green of Banking Circle concludes, the gap will only close if regulators and the industry move together:

> **"From regulators, it means treating banks as partners in risk assessment rather than the default enforcement layer. Shared intelligence models, including law enforcement task forces that pool industry data, show what that collaboration could look like. From industry, it means making better use of the data and technology already available to make screening more precise rather than more binary, instead of waiting for regulation to force the change. Closing the gap needs both sides moving at the same time."**
>
> Patrick Green, Chief Compliance Officer, **Banking Circle**

IN BRIEF

1. The impact of the European Union Instant Payments Regulation has been felt throughout the payments industry.
2. The IPR requires a shift from one-time transaction screening to periodic customer screening.
3. The quality of the underlying client data and sanction datasets is particularly important under this new screening situation.

Is your organisation ready for the Instant Payments Regulation?

Speak with a Dow Jones Risk & Compliance expert about what it means for your sanctions screening and how we can support you.

TALK TO AN EXPERT

DOW JONES
RISK & COMPLIANCE

Dow Jones Risk & Compliance offers best-in-class data, technology, insight and services to fight financial crime, manage third-party and supply chain risk and ensure trade and sanctions compliance. Dow Jones Risk & Compliance solutions are designed to meet the requirements of global organizations. We address the needs of senior leaders who require insight and benchmarking, compliance professionals who define policies and design programs, and operational teams who need reliable, effective and efficient solutions.

pa eu **The Payments Association EU**

DOW JONES RISK & COMPLIANCE **Dow Jones Risk & Compliance**