SPOTLIGHT ON EU PAYFACS

Understanding PSD3, Requirements, and How European Union (EU) Reinvents PayFacs

A Spotlight on New EU Payment Service Directive, Requirements, and Why It Matters

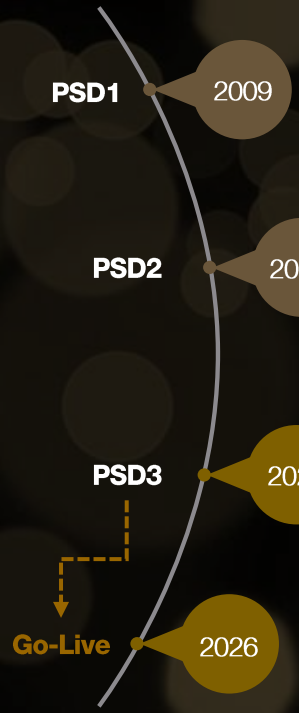
StratisAdvisory

RISK | STRATEGY | CYBER | COMPLIANCE MANAGEMENT

Payment Facilitators under the EU Payment Service Directives

The payment facilitation industry is rapidly evolving. European Union (EU) region is not new to the ever-changing landscape of regulatory frameworks to address risks and build a future-proof environment of payment facilitators. One of the most current reforms is the transition from Payment Service Directive 2 (PSD2) to PSD3. These entail modernization in the payment ecosystem, enhance consumer protection, and combat financial crimes more effectively. The following provides insight into the PSDs:

Progression of EU's PSDs



PSD1 — PSD1 was implemented on November 1, 2009 with the main objective to create a single internal market for payments in the region. PSD1 introduced licensing for payment institutions and enhanced transparency in fees and timeframes.

PSD2 — PSD2 came into effect on January 13, 2018 with the goal to enhance security, competition, and innovation. This implemented Strong Customer Authentication (SCA) and created roles such as Account Information Service Providers (AISP) and Payment Initiation Service Providers (PISP).

PSD3 — PSD3 aims to modernize PSD2 and address emerging risks. This new directive is still under review by EU institutions with the final versions expected to be available by early 2025. One of the highlights on changes include alignment with the Digital Operational Resilience Act (DORA), which was enacted last January 2023 to ensure operational resilience and cybersecurity.

Go-Live — The expected entry into force of PSD3 is mid-to-late 2026 after an 18-month transition with full compliance deadline likely to happen by 2027.

PSD3 Key Regulatory Shifts

Stronger Customer Authentication

Expansion of SCA requirements to scope more transaction and business types.

Mandatory Name Matching

Verification of payee's name matching the International Bank Account Number (IBAN) before processing transfers.

Fraud Monitoring and Data Sharing

Real-time monitoring of fraud patterns must be in place and conduct annual fraud training for employees.

Operational Resiliency and Cybersecurity

Alignment with DORA and institutions are required to submit annual assessments of operational and security risk.

Expanded Consumer Protection

Enhanced transparency in account statements and data usage and clearer disclosures on ATM charges.

The PSDs Have Increased Oversight of Payment Facilitators

The implementation of PSD2 and the upcoming PSD3 have significant strategic, economic, and regulatory changes in the EU. The PSDs reshape the responsibilities of PayFacs, Fintech, merchants, and consumers. The following is a breakdown on the evolution of PSDs across the key areas that matter most to PayFacs.

KEY AREAS	PSD1	PSD2	PSD3 (Proposed)
Payment Facilitator Role	Not defined	Recognized via AISP and PISP.	Clearly scoped under unified licensing with direct access to payment systems in EU.
Licensing	Introduced Payment Institution (PI) licensing.	Added AIS and PIS services.	Merges PSD2 with E-Money Directive. All PSPs must reapply for authorization.
Fraud Controls	Basic transparency and liability rules are applied.	Added SCA and liability caps.	Adds IBAN-name matching, real-time fraud data sharing, and liability shift for fraud.
Authentication	Not mandated	Required 2-factor authentication for digital or electronic payments.	Introduces flexible SCA and allows accessibility for vulnerable users in EU.
Open Banking	Not addressed	Mandated API access for third-party providers with user consent.	Requires standardized APIs, user dashboard, and fallback interface removal in EU.
Cybersecurity	Minimal guidance	Required incident reporting and risk controls.	Alignment with DORA and mandates resilience testing and third-party risk management.
Training and Awareness	Not required	Introduced staff awareness training.	Mandates annual fraud training for staff and consumer education campaigns are encouraged.

PayFacs in Germany, Ireland, The Netherlands, and Lithuania

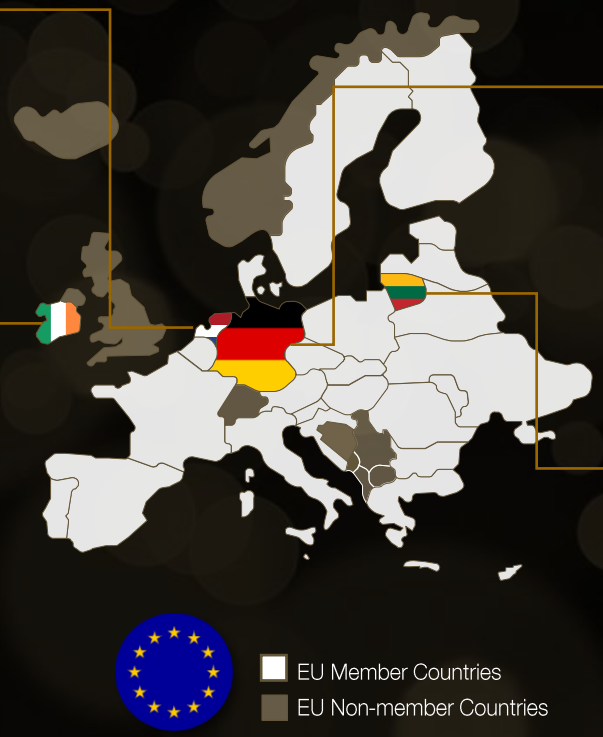
As of 2025, 4 EU-member states have taken a proactive approach to align with PSD2 and prepare for PSD3. The regulatory shift is not just about ticking compliance checklist, but a move to reinvent how PayFacs operate, manage risk, and build trust to its customers. Beyond PSD2, PSD3 aims to combat fraud, enhance consumer rights, and level the playing field for non-bank payment service providers.

The Netherlands

- Dutch banks are embedded with fraud screening and sanctions checks to align with 24/7 Single Euro Payments Area (SEPA) instant payment initiative.
- The Netherlands pioneered implementation of Verification of Payee (VOP), which now expands to all credit transfers nationally.

Ireland

- Irish payment service providers (PSPs) are piloting machine learning models to detect real-time fraud and conduct transaction risk analysis.
- Open banking dashboards are deployed by banks, which is a key requirement on PSD3.



Germany

- Germany is proactively rolling out VOP across all credit transfers and not limiting to instant payments to meet PSD3's fraud prevention mandates.
- Fraud liability frameworks are embedded to internal policies to reflect PSD3's liability shift for impersonation and social engineering fraud.

Lithuania

- Lithuania PSPs are actively participating in EU-wide fraud intelligence networks, which is a requisite in PSD3.
- Lithuania mandates annual risk assessments and incident reporting for all licensed entities as part of DORA alignment.

Jurisdiction-Based AML/CFT Assessment: Germany

When it comes to assessing AML/CFT, Germany adopts a risk-based approach tailored to PayFacs. While activities include safeguarding reviews into AML/CFT controls, and leveraging technologies for real-time monitoring, Germany continue to refine frameworks to align with the ever- changing regulatory landscape. The following provides insight into Germany's approach to payment facilitation:

EU Member Countries
EU Non-member Countries

Germany

Local Concepts

- ***Geldwäschegesetz (GwG).*** Germany's Anti-Money Laundering Act, formally known as the Act on the Detection of Proceeds from Serious Crimes. Originally enacted in 1993, it has since been updated to reflect evolving EU regulations such as the 2024 AML package and upcoming PSD3 implementation.
- ***Verpflichtete. R****efers to obliged entities under the GwG in which PayFacs are legally required to implement AML/CFT controls among other financial institutions.*
- *Risikobewertung.* The German term for risk assessment and refers to the process of identifying, analyzing, and evaluating potential risks that could impact the entity.

Assessment Industry Standards

1. Conduct a Risikobewertung.
2. Implement internal safeguards such as appointing an AML Officer (Geldwäschebeauftragter), establishing written policies for customer onboarding and verification, transaction monitoring, and staff training and audit trails are in place.
3. Verify identity of merchants and beneficial owners through customer due diligence (CDD) and enhanced due diligence (EDD).
4. Monitor transactions for spikes or unusual payment patterns and screen against EU and UN sanctions list.
5. File reports if there are any suspicious activities via Financial Intelligence Unit Germany.
6. Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) or the Federal Financial Supervisory Authority of Germay requires PayFacs for daily reconciliation of client funds and submit safeguarding risk assessments annually.

Relevance to Payment Facilitators

BaFin
Bundesanstalt für Finanzdienstleistungsaufsicht

BaFin plays a critical role to PayFacs on the following aspects:

- Licensing
- Safeguarding Rules
- AML/CFT Compliance

Jurisdiction-Based AML/CFT Assessment: The Netherlands

While Germany's AML/CFT assessments are highly structured and with strong emphasis on daily funds reconciliation, The Netherlands leads a data-driven regime with their AML/CFT assessments heavily relying on standardized templates, real-time transaction monitoring, and UBO verification. PayFacs are expected to have audit-ready documentation and aligns with Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) or the Dutch Anti-Money Laundering and Anti-Terrorist Financing Act.

EU Member Countries
EU Non-member Countries

The Netherlands

Local Concepts

- ***Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft).*** The Dutch Anti-Money Laundering and Anti-Terrorist Financing Act, which was enacted on August 1, 2008.
- ***Risicoanalyse.*** *R*efers to risk analysis and a process to identify, assess, manage, and mitigate potential risks.
- *Trasnactiemonitoring. T*ransaction monitoring which is a core process of AML/CFT compliance and involves continuous tracking, analysis, and evaluation of transactions to detect unusual or suspicious activities.

Assessment Industry Standards

1. Conduct a Systematic Integrity Risk Analysis (SIRA) that is tailored based on the merchant type, transaction volumes, and delivery models.
2. Verify identity of merchants and beneficial owners through customer due diligence (CDD) and enhanced due diligence (EDD) depending on risk levels.
3. Conduct transactiemonitoring.
4. File reports if there are any suspicious activities via Financial Intelligence Unit Netherlands.
5. Appoint a Wwft Compliance Officer.
6. De Nederlandsche Bank (DNB), is the financial supervisory authority in the Netherlands, which requires PayFacs standardized risk scoring tools and real-time monitoring for fund flows and AML alerts.

Relevance to Payment Facilitators

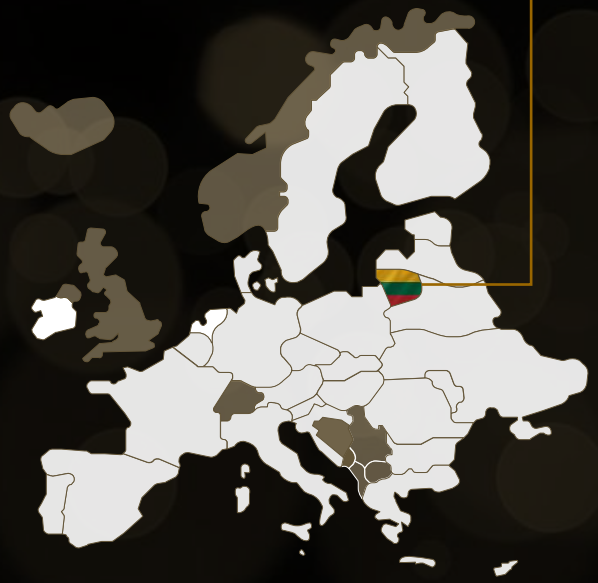
DeNederlandscheBank
EUROSYSTEEM

DNB is vital to PayFacs on the following aspects:

- Licensing
- Reporting Thresholds
- AML/CFT Compliance

Jurisdiction-Based AML/CFT Assessment: Lithuania

Generally, Lithuania fosters a friendly rapport to FinTechs with the Bank of Lithuania supporting API-based fund tracking and pre-licensing consultations. PayFacs are benefitting from cross-border licensing support and mandatory annual Systematic Integrity Risk Analysis (SIRA) submissions.



EU Member Countries
EU Non-member Countries

Lithuania

Local Concepts

- *Pinigų plovimo ir terorizmo finansavimo prevencijos įstatymas.* Lithuania's Law on the Prevention of Money Laundering and Terrorist Financing, which was enacted on June 19, 1997 and has undergone multiple revisions to align with EU AML Directives.
- *Įpareigotieji subjektai.* Refers to Lithuania's term for obliged entities required to implement AML/CFT measures.

Assessment Industry Standards

1. Annual SIRA is mandatory in Lithuania and must cover merchant onboarding risks, transaction flows, and geographic or cross-border risks.
2. Conduct CDD and EDD to identify UBOs, business nature, complex ownership structures, and high-risk persons such as politically exposed persons.
3. Monitor unusual transaction patterns through transaction monitoring with the use of API-based tools.
4. File reports on suspicious transactions to Financial Crime Investigation Service (FNTT).
5. Embed sanctions screening into onboarding and monitoring workflows.
6. Appoint a compliance officer responsible for AML/CFT.
7. Comply with GDPR and AML laws on retention.

Relevance to Payment Facilitators

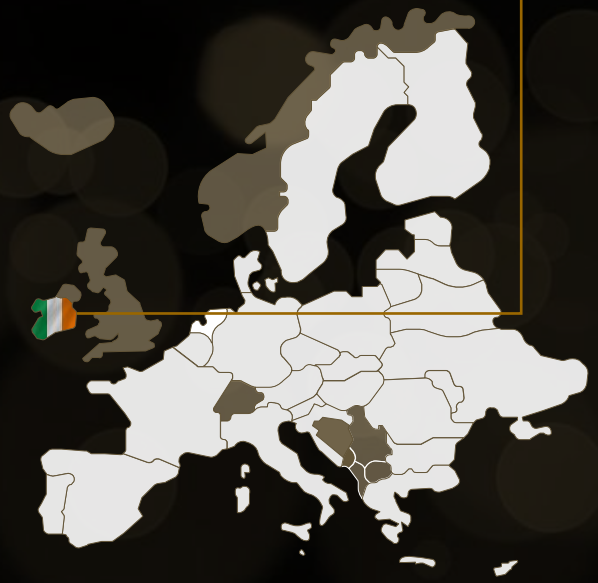
LIETUVOS BANKAS
EUROSISTEMA

The Bank of Lithuania is the primary supervisory authority with oversight on:

- Licensing
- Safeguarding Control
- AML/CFT Compliance

Jurisdiction-Based AML/CFT Assessment: Ireland

Ireland adopts an Enterprise-Wide Risk Assessment (EWRA), which is a principles-based approach to its AML/CFT assessment framework. Ireland's AML/CFT regime is mandated in the Criminal Justice Acts 2010-2021 (Money Laundering and Terrorist Financing) and PayFacs are considered obliged entities to implement EWRA. The framework focuses on board accountability, ethical conduct, residual risk tolerance, and documented operational protocols.



EU Member Countries
EU Non-member Countries

Ireland

Local Concepts

- *Enterprise-Wide Risk Assessment (EWRA).* Ireland's foundational AML/CFT compliance framework mandated by the Criminal Justice (Money Laundering and Terrorist Financing) Acts 2010-2021 and enforced by the Central Bank of Ireland.
- ***Risk Appetite Statement.*** PayFacs operating in Ireland can justify risk-based decisions in onboarding and transaction monitoring through this. It also helps demonstrate board-level oversight and governance maturity, align with its AML/CFT obligations, and support regulatory engagement.

Assessment Industry Standards

1. Conduct a holistic review of AML/CFT risks through EWRA that will cover customer types, embedded payments, channels, and geographic exposure.
2. Conduct CDD and EDD to identify UBOs, business nature, complex ownership structures, and high-risk persons such as politically exposed persons.
3. Monitor unusual transaction patterns and maintain audit trails and escalation flows.
4. Suspicious Transaction Reports (STRs) must be filed to An Garda Síochána (Irish Police) and Revenue Commissioners through the goAML portal.
5. Appoint AML/CFT Compliance Officer and Money Laundering Reporting Officer (MLRO).
6. Compliance with retention rules for transaction logs, risk assessments, and CDD documentation.

Relevance to Payment Facilitators

Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

Central Bank of Ireland has the regulatory oversight for PayFacs in Ireland for:

- Licensing
- Safeguarding Control
- AML/CFT Compliance

Safeguarding Reviews and Global Assessments

Under PSD3, the concept of diversification of safeguarding channels introduces a more robust framework of protecting client funds, especially for PayFacs. This entails a strategic shift from PSD2's flexible approach to risk-sensitive, regulator-driven model.

Core Safeguarding Principles in the EU

Fund Segregation

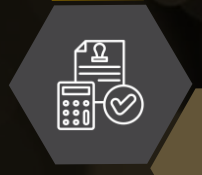
Client funds must be held in accounts separate from operational funds. Entities must also use credit institutions or safeguard directly with banks under PSD3.

Diversification of Channels

PSD3 introduced a requirement to diversify safeguarding methods to reduce concentration risks.

Daily Reconciliation

Reconciliation of client balances and fund movements is a mandatory task daily, to detect anomalies and shortfalls.



Change Notification

In PSD3, entities are obliged to notify regulators in advance of any material changes to safeguarding setups.

Operational Continuity

Institutions must establish and maintain incident response plans to protect client funds during disruptions.

Diversification Impact on PayFacs

1. **Operational Adjustment.** Redesigning of fund flows to support multi-bank safeguarding and the need to automate reconciliation tools to track diversified holdings. PayFacs must avoid placing all safeguarded funds with one credit institution.
2. **Governance.** Board oversight must align with the safeguarding diversification as part of their risk appetite and compliance team's need to document justification for chosen safeguarding mix.
3. **Cross Border Complexity.** Jurisdictional alignment must be ensured on PayFacs operating in multiple EU states. Portability and scalability of diversification must be considered across EU states.

The fragmented regulatory landscape in EU alone mounts a challenging patch for PayFacs in operating multiple geographies to unify AML/CFT, safeguarding, and operational risk controls. Operational structuring blended with optimized and agile regulatory landscape mapping play a critical role in helping PayFacs establish a regulator-ready infrastructure tailored to jurisdictional refinements.

Discover what Stratis Advisory can do for you

Compliance Program Development

An enterprise AML and sanctions compliance program is founded on the five (5) pillars of internal controls, training, a compliance officer, independent review and customer due diligence. Stratis can help you develop, evaluate and implement a scale-appropriate AML and sanctions compliance program suitable for your business model and regulatory or partner-based environment, ensuring that you stay ahead of evolving regulations, guidance, and enforcement.

AML Independent Review

Whether operating as a regulated financial institution or through various bank, payment, or lending partnership models, typically an annual review of your AML and sanctions programs is a requirement. As Stratis serves a portfolio of global regulated and unregulated companies, Stratis can help you with performing your required AML and sanctions review on a scale and risk-appropriate basis to satisfy your statutory requirement, but also any requirement(s) from your banking partner.

TempCCO® Outsourced Compliance Function

Developing a compliance program is the just the initial step in operating as a Payfac, regulated financial institution, or as a partner of one. Operationalizing your compliance program is critical to maintain compliance, bank accounts, and for successful audits and examinations. Depending on the life cycle of your organization, Stratis can provide you with on-going risk, strategy, and compliance support under our TempCCO® outsourced compliance function to assist you while launching, scaling, or optimizing your compliant program.

Stratis Advisory | 1.415.352.1060 | www.stratisadvisory.com | info@stratisadvisory.com