Economic Crime Outlook Europe 2026

Strategic Intelligence Report on Fraud, Corporate Risks, Supply Chain Crime and International Economic Threats.
Prepared in the style of an operational intelligence assessment for decision-makers, law firms, insurers and international companies.

Europe is currently experiencing a significant transformation in the field of economic crime. Traditional fraud models are increasingly merging with cyber-enabled operations, supply-chain manipulation, identity misuse and international corporate deception. At the same time, organised criminal structures are becoming more professional, more international and significantly more adaptive. Especially affected are: international logistics companies, manufacturing industries, insurance providers, investment structures, compliance departments, medium-sized businesses and cross-border corporate networks. This report summarises current developments, operational observations and strategic risk patterns relevant for 2026.

1. Supply Chain Fraud & Phantom Carrier Networks

Cargo theft in Europe is increasingly shifting from physical attacks towards digital infiltration and identity manipulation. Criminal groups now frequently impersonate legitimate transport companies, manipulate freight forwarding communication and intercept valuable goods before transportation even begins. Particularly affected regions include Germany, Benelux, France, Poland and parts of Eastern Europe. Current observations indicate: rapid increase of fake carrier registrations, use of cloned corporate identities, fraudulent transport insurance documentation, targeted attacks against high-value electronics and pharmaceuticals, international coordination via encrypted communication platforms. Many affected companies discover the fraud only after complete disappearance of the shipment.

2. Deepfake & AI-Enabled Fraud

Artificial intelligence is increasingly being used for economic crime. Voice cloning, manipulated video conferences and AI-generated executive impersonation attacks are becoming more common. Attackers use: deepfake voice technology, AI-generated profile identities, synthetic LinkedIn personas, fake legal correspondence and automated phishing structures. The financial damage can be substantial, especially when internal payment processes and trust-based approval structures are exploited.

3. Corporate Espionage & Insider Risks

Insider threats remain one of the most underestimated corporate risks in Europe. In many cases, sensitive data is not stolen by external hackers but by internal actors, subcontractors or temporary staff members with legitimate system access. Common targets include: customer databases, pricing structures, technical documentation, supplier contracts and research and development data. Particularly vulnerable are internationally operating companies with decentralised structures and weak compliance coordination.

4. International Due Diligence Risks

Cross-border investments increasingly require enhanced investigative due diligence. Investors and corporate decision-makers often face: hidden ownership structures, sanctions exposure, unverified beneficial owners, reputation laundering and complex offshore networks. Especially in high-risk jurisdictions, open-source intelligence alone is often insufficient. Human intelligence, local verification and operational field inquiries remain essential.

5. Outlook for 2026

The operational complexity of economic crime in Europe will continue to increase throughout 2026. The convergence of cybercrime, organised crime and economic fraud is expected to intensify further. Companies should therefore strengthen: internal compliance systems, supply chain verification, executive protection structures, digital forensic readiness and international risk intelligence capabilities. Preventive intelligence and rapid-response investigations will become increasingly important for damage limitation and reputational protection.

Strategic Risk Overview

Risk Area	Trend 2026	Operational Risk Level
Supply Chain Fraud	Strong Increase	High
AI-Enabled Fraud	Very Strong Increase	Critical
Corporate Espionage	Moderate Increase	High
Internal Fraud	Stable Increase	Medium-High
Cross-Border Scam Structures	Strong Increase	High

Detegere – Corporate Intelligence & Economic Crime Investigations