# Managing payment fraud in the Baltic states

## Strategies to achieve and sustain a state of equilibrium

January 2026

# What's inside

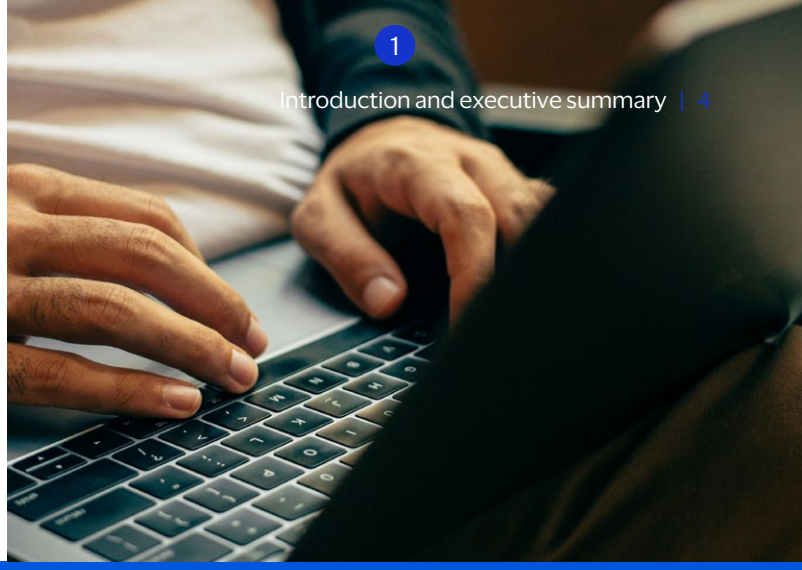


# Introduction and executive summary

The Baltic states have embraced digital payments at a dizzying pace. Both card and account-to-account (A2A) transfers have become embedded in everyday banking, enabling peer-to-peer payments, bill settlement and, increasingly, e-commerce transactions.

This shift has delivered significant benefits in terms of speed and convenience for consumers and businesses alike. But the rapid adoption of real-time payments has contributed to a material shift in fraud patterns and risk dynamics. Today, consumer payment behaviours are evolving, attack surfaces are expanding, and fraud techniques are becoming increasingly sophisticated.

In this paper, Visa Consulting & Analytics (VCA) provides an assessment of the current fraud and risk environment in Estonia, Latvia, and Lithuania. Drawing on VisaNet transaction intelligence, findings from a programme of recent interviews with senior risk practitioners, in-depth consumer surveys, and regulatory insights, we look at how a new state of equilibrium can be achieved and sustained – enabling the industry to deliver the speed and convenience that customers expect, deploying robust security controls without generating excessive false positives, and achieving a measurable return on investments from fraud prevention initiatives.



## Four themes that characterise payment fraud in the Baltics

Our analysis reveals four fraud-related themes that stand out across the Baltics:

**The real-time frontier and its downsides** – Baltic consumers and businesses have embraced real-time payments at a scale few regions can match. Instant account-to-account (A2A) transfers, deeply integrated into everyday banking channels, have become the default for peer-to-peer (P2P) payments, bill settlement, and increasingly, e-commerce. Yet the same speed and finality that power economic efficiency have also accelerated fraud.

**The personalisation of fraud and its industrialisation** – The professionalisation of fraud is accelerating. A recent survey of 114 global fraud executives found that 96% expect the use of artificial intelligence (AI) among fraudsters to increase, with two-thirds rating fraudster sophistication as equal to or greater than that of solution providers and 76% viewing AI-powered detection as the most promising defence.[1] Meanwhile in our programme of interviews (see page 28), Baltic practitioners report instances of native-language scam calls generated synthetically using AI, deepfake voice cloning, and multi-step social-engineering campaigns coordinated across phishing, SMS, and high-pressure phone calls.

**Digital leadership and its vulnerabilities** – Estonia, Latvia, and Lithuania rank among Europe's most advanced digital payment environments, with near-universal banking penetration and SEPA Instant adoption dating to 2017. Yet this digital maturity has created new vulnerabilities. The fraud mix is shifting: from traditional card-not-present (CNP) fraud toward A2A and Authorised Push Payment (APP) scams that weaponise speed, social engineering, and regulatory gaps. Investment scams and telephone fraud (vishing) now dominate losses across all three markets. While A2A fraud rates have recently improved, the Baltics still generate a disproportionate share of EU fraud by value – at roughly three-to-five times their volume share.

**Regulatory responses and their consequences** – The regulatory environment is evolving, pressure is mounting, and obligations are changing. For example, the EU's Instant Payments Regulation (IPR) mandated Verification of Payee (VoP) from October 2025, the Digital Operational Resilience Act (DORA) imposed information and communication technology (ICT) resilience standards from January 2025 and, scheduled for 2026, PSD3/PSR is set to shift liability for authorised fraud onto payment service providers, expand reimbursement obligations, and require near-real-time fraud data sharing. Meanwhile, both Latvia and Lithuania have issued national fraud-risk guidelines mandating unified governance, dedicated Fraud Prevention Officers, and formalised complaint handling. The cumulative effect is a decisive shift from 'best efforts' to 'accountability by design'.

[1] Datos Insights, Five Forces Reshaping Fraud Prevention by 2030, 2025: https://datos-insights.com/blog/global-fraud-prevention-trends-2030

## What practitioners and consumers are telling us

Between September and November 2025, Visa interviewed senior risk practitioners – chief risk officers, heads of fraud, compliance leaders – from issuers, acquirers, payment service providers, industry associations, and regulatory bodies across the Baltics. The interviews reveal a sector in transition: fraud prevention is universally a top priority, yet most institutions acknowledge fragmented technology stacks, siloed data architectures, and limited real-time integration across channels.

Practitioners consistently reported that A2A fraud now exceeds card fraud in both volume and value, that social-engineering and investment scams dominate losses, and that regulatory uncertainty around PSD3 and the rising sophistication of AI-enabled attacks are the most pressing challenges. Regulators describe the current situation as a 'pandemic of fraud' and stress that legislation must evolve to enable banks to block suspicious transactions proactively, even when strong customer authentication is present. The good news is that collaboration is also accelerating – with industry working groups, telecom partnerships to block spoofed calls, cross-institution intelligence-sharing platforms, and closer coordination with national Computer Emergency Response Team (CERTs) all gaining momentum.

Meanwhile, a Visa-commissioned Ipsos consumer survey of 1,200 Baltic citizens in June 2025 confirms both the scale of the problem and significant awareness gaps – more than half (51%) say they had encountered fraud attempts in the past year, yet only 12% of victims reported incidents, and more than 60% were unaware that card payments offer more protection than A2A transfers.

## Strategies for achieving equilibrium

Although collaboration and cooperation are among the most effective strategies to achieve equilibrium, there is a strong onus on all players to evolve their approach to fraud management. But, with every player having a different risk profile, there will be no one-size-fits-all remedies.

To help institutions assess their current capabilities and chart a path forward, VCA has developed a diagnostic framework tailored to organisational specifics. The approach begins with a high-level maturity assessment using broad benchmarks (overall fraud rates, approval rates, latency), then advances to a detailed scorecard with granular metrics, like fraud detection rates, false-positive ratios, manual-review volumes, and customer friction indicators. It then provides tailored recommendations and technology roadmaps and enables institutions to adopt continuous improvement tracking – which transforms diagnostics into a living tool for ongoing monitoring, peer benchmarking, and strategic adjustment.

> "In today's world there will be some collateral damage from blocking, and that's fine. That's the new reality where we're living."

> "We are always one or two steps behind the fraudsters."

## Charting a path to sustainable fraud prevention

As we explore in this paper, the forces of change are set to escalate and accelerate. So, the fraud management response must be equally agile and dynamic. And, looking ahead, we envisage that six forces will define fraud prevention:

1. The AI arms race
2. The continued rise of A2A and instant payments
3. The growth of cross-border flows
4. Tightening regulation and expanded liability
5. Rising consumer expectations
6. The proliferation of new payment rails and digital assets

Against this background, Baltic institutions typically describe their current readiness as 'below mid-level' in some areas. Yet they tend to express cautious optimism that meaningful progress is achievable within two to three years if investments in unified data, AI-driven controls, cross-sector collaboration, and regulatory alignment continue.

Achieving sustainable fraud prevention in the Baltics requires a layered, AI-enabled approach that integrates real-time transaction monitoring and customer interaction, adaptive authentication, tokenization, beneficiary risk scoring, consortium data intelligence, and human-in-the-loop review. Institutions that deploy these controls across both card and A2A rails can approve more legitimate payments, intercept scams earlier, and do both with lower unit costs – while maintaining a positive customer experience by balancing strong security with frictionless payment journeys.

The path forward demands collaboration within institutions, across institutions, and between industry and regulators.

## REGULATORY CONTEXT AND NEW DEVELOPMENTS IN CARD SCHEME RULES

**01** **1 May 2024** | Entry into force

**National Guidelines (LT) - Fraud Prevention Guidelines**

**Authority** Lietuvos Bankas
**Focus** Fraud-risk governance and minimum controls for PSPs and e-money institutions.
**Impact** Stronger monitoring, mandatory loss reporting, and alignment with national Fintech and cyber strategy.

**02** **30 Dec 2024** | Entry into application

**MiCA (Markets in Crypto Assets Regulation)**

**Authority** European Commission, ESMA
**Focus** Uniform EU market rules for crypto-assests.
**Impact** Support market integrity and financial stability of crypto-assets and by ensuring consumers are better informed about their associated risks.

**03** **9 Jan 2025** | 1st obligations entered to application

**Instant Payments Regulation (IPR) — 1st Obligation: Receive Payments (Euro-area PSPs)**

**Authority** European Commission, European Central Bank (ECB)
**Focus** Mandatory instant-payment receipt for all euro-area PSPs.
**Impact** Enables 24/7 payment acceptance across the EU; foundation for VoP adoption.

**04** **17 Jan 2025** | Entry into application

**Digital Operational Resilience Act (DORA)**

**Authority** The European Union, National Competent Authorities (e.g., Latvijas Banka, Lietuvos Bankas, Eesti Pank)
**Focus** Ensures ICT resilience and mandatory incident reporting.
**Impact** Brings harmonisation to rules relating to operational resilience for the financial sector, applicable to 20 different types of financial entities and ICT third-party service providers.

**05** **19 May 2025** | Published

**National Guidelines (LV) - Guidelines for Monitoring, Managing and Mitigating the Risk of Financial Fraud**

**Authority** Latvijas Banka, Finance Latvia Association
**Focus** Unified fraud-management standards and mandatory incident reporting.
**Impact** Stronger audit regimes; real-time fraud data sharing with CERTs.

**06** **1 Oct 2025** | Full application

**Visa Acquirer Monitoring Program (VAMP) — Enforcement Phase**

**Authority** Visa Global
**Focus** Combines fraud, dispute, and enumeration metrics under unified "VAMP ratio."
**Impact** Enables real-time acquirer risk monitoring and mandatory remediation.

**07** **9 Oct 2025** | 2nd obligations entered to application

**Instant Payments Regulation (IPR) — 2nd Obligation: Send Payments & Verification of Payee (VoP)**

**Authority** European Commission, ECB
**Focus** Mandatory instant-payment send for all euro-area PSPs; Requires IBAN name-check before instant payments.
**Impact** Critical step to reduce misdirected and fraudulent A2A payments.

**08** **2026/27** | Expected to enter into application

**PSD3 / PSR Package (Payments Services Directive & Regulation)**

**Authority** European Commission, Council, Parliament, EBA
**Focus** Expands anti-fraud obligations and consumer reimbursement rights.
**Impact** Shifts fraud liability to PSPs; strengthens cross-border data sharing.

**09** **9 Jan - 9 July 2027** | Receive transfer and send in euro

**Instant Payments Regulation (IPR) Full Compliance (Non-Euro PSPs)**

**Authority** European Commission, ECB
**Focus** VoP and instant-payment rules extended to all EU PSPs.
**Impact** Achieves full EU harmonization and end-to-end instant-payment protection.

**10** **Late 2027** | Expected to enter into application

**FIDA (Financial Data Access Regulation)**

**Authority** European Commission, Council, Parliament
**Focus** Expands open-finance scope beyond payments.
**Impact** Enables secure data-sharing for advanced fraud and risk analytics.

# Setting the scene – high levels of digitisation, with tightening regulation, and a framework for closer cooperation

## A digitally advanced payments environment

The Baltic region stands out as one of Europe's most digitally advanced payments environments. All three countries have achieved near-universal banking penetration (Estonia: 99%, Latvia: 95%, Lithuania: 99%),[2] and their populations are prolific users of electronic payments. Debit cards are the overwhelming preference, accounting for 71-93% of cards in circulation and 78-94% of card payment volume.[3] Credit card penetration remains modest, reflecting a strong cultural aversion to debt and a regulatory environment that prioritizes financial security and responsible lending.

The adoption of instant payments is a defining feature of the Baltic landscape. Estonia, Latvia, and Lithuania were among the first in the EU to implement SEPA Credit Transfer Instant (SCT Inst) in 2017, and today, real-time A2A transfers via bank apps are the norm for both P2P and bill payments. Unlike Sweden's Swish, Norway's Vipps or Denmark's MobilePay, none of the Baltic states have a single dominant P2P wallet.

Instead, instant A2A payments are integrated into bank channels, reflecting a highly interoperable, bank-driven ecosystem. As of January 2025, 13 banks in Latvia participate in SCT Inst,[4] and the system is used for everything from government payments to everyday consumer transfers. And, for the second half of 2024, Latvia recorded the highest share of credit transfers among all eurozone countries, with 36% of all non-cash payments at the national level made via credit transfers.[5]


[2] World Bank Group, Global Findex Database: https://www.worldbank.org/en/publication/globalfindex
[3] Data from the respective central banks of the three Baltic states (See: https://www.lb.lt/en/payments-statistics-1, https://statistika.eestipank.ee/#/en/p/FINANTSSEKTOR/620, and https://statdb.bank.lv/lb/Data/282)
[4] Latvijas Banks, EKS Participants: https://www.bank.lv/component/content/article/3833-latvijas-bankas-elektroniska-kliringa-sistema
[5] European Central Bank, Payments statistics: second half of 2024, 2025: https://www.ecb.europa.eu/press/stats/paysec/html/ecb.pis2024h2-5ada0087d2.en.html
[6] Data from the respective central banks of the three Baltic states (See: https://www.lb.lt/en/payments-statistics-1, https://statistika.eestipank.ee/#/en/p/FINANTSSEKTOR/620, and https://statdb.bank.lv/lb/Data/282)
[7] Euro News, Keeping cash across Europe, 2025: https://www.euronews.com/business/2025/10/05/keeping-cash-across-europe-which-countries-use-the-most
[8] Invest Lithuania, The Fintech Landscape in Lithuania, 2025: https://investlithuania.com/wp-content/uploads/LT-fintech-report-2024-2025.pdf
[9] Emerging Europe, Estonia cracks down on crypto to protect its status as a global tech hub, 2023: https://emerging-europe.com/analysis/estonia-cracks-down-on-crypto-to-protect-its-status-as-a-global-tech-hub
[10] ThreatMark, The Baltics Under Pressure: RTP, Scams, and Smarter Fraud Defense, 2025: https://www.threatmark.com/baltics-under-pressure/
[11] Fintech Nordics, Nordics and Estonia to Roll Out Offline Card Payments Amid Rising Cybersecurity Threats, 2025: https://fintechnordics.com/8720/fintechfinland/nordic-baltic-offline-payments/
[12] Commsrisk, Baltic Telcos Hail Blocks on Spoofed Inbound International Calls, 2024: https://commsrisk.com/baltic-telcos-hail-blocks-on-spoofed-inbound-international-calls/

Debit cards are used for both in-store and online purchases, with contactless functionality now standard (over 90% of cards and POS terminals support NFC).[6] Bill payments are typically made via credit transfers or instant A2A, with cards rarely used for recurring bills. Cash usage, while declining rapidly, remains relevant – ranging from around 39% of transaction volume in Estonia, to 45% in Latvia, to 54% in Lithuania.[7]

The region's fintech sector is also vibrant and growing. Lithuania, and especially Vilnius, has become the EU's largest fintech centre by number of licensed firms (282 in 2024), serving over 30 million EU customers, supported by a proactive regulator, dedicated ecosystem initiatives (e.g., Fintech Hub LT, ROCKIT), a robust talent pool, and a business-friendly environment.[8] Estonia and Latvia also foster dynamic fintech and digital banking sectors, with Estonia previously hosting the world's largest number of registered virtual asset service providers (VASPs) before regulatory tightening.[9]

Economic growth and fintech-driven retail investing have expanded opportunities for self-directed wealth management but have also increased exposure to investment scams – which is now among the top fraud categories in the region – along with telephone fraud.[10]

Meanwhile, the wider geopolitical context has heightened the focus on payment system resilience and crisis readiness. Estonia and Latvia, in partnership with Nordic countries, are developing offline-capable card payment systems enabling encrypted transactions to be processed in the event of internet and power outages, including those caused by sabotage. Sweden plans a full offline rollout of its solution by July 2026, while Denmark and Norway already support multi-day PIN-based contingencies.[11]

In terms of cross-sector collaboration, telcos now block spoofed international calls, stopping tens of thousands of vishing attempts monthly. This shows the value of financial–telecom collaboration, including 24/7 hotlines linking fraud teams and network centres.[12]

## Credit transfers in the non-cash payments mix among eurozone countries (2024 H2):[13]

**35.9%**
in Latvia – top 1

**35.1%**
in Estonia – top 2

**15.4%**
in Lithuania

**22.6%**
in Eurozone

[6] Data from the respective central banks of the three Baltic states (See: https://www.lb.lt/en/payments-statistics-1, https://statistika.eestipank.ee/#/en/p/FINANTSSEKTOR/620, and https://statdb.bank.lv/lb/Data/282)
[7] Euro News, Keeping cash across Europe, 2025: https://www.euronews.com/business/2025/10/05/keeping-cash-across-europe-which-countries-use-the-most
[8] Invest Lithuania, The Fintech Landscape in Lithuania, 2025: https://investlithuania.com/wp-content/uploads/LT-fintech-report-2024-2025.pdf
[9] Emerging Europe, Estonia cracks down on crypto to protect its status as a global tech hub, 2023: https://emerging-europe.com/analysis/estonia-cracks-down-on-crypto-to-protect-its-status-as-a-global-tech-hub
[10] ThreatMark, The Baltics Under Pressure: RTP, Scams, and Smarter Fraud Defense, 2025: https://www.threatmark.com/baltics-under-pressure/
[11] Fintech Nordics, Nordics and Estonia to Roll Out Offline Card Payments Amid Rising Cybersecurity Threats, 2025: https://fintechnordics.com/8720/fintechfinland/nordic-baltic-offline-payments/
[12] Commsrisk, Baltic Telcos Hail Blocks on Spoofed Inbound International Calls, 2024: https://commsrisk.com/baltic-telcos-hail-blocks-on-spoofed-inbound-international-calls/
[13] European Central Bank, Payments statistics: second half of 2024, 2025:https://www.ecb.europa.eu/press/stats/paysec/html/ecb.pis2024h2-5ada0087d2.en.html

## Closer scrutiny, tighter regulation, and shifting liabilities

The regulatory environment in the Baltics is characterised by a decisive shift from 'best efforts' to 'accountability by design'. The implementation of PSD2 in all three countries opened bank-held customer data and systems to third-party providers, fostering innovation and improving consumer protection. The Instant Payment Regulation (IPR) requires euro-area payment service providers (PSPs) to send instant payments and provide VoP checks from October 2025, with equality-of-charges rules for cross-border payments.

Meanwhile, the Digital Operational Resilience Act (DORA), effective from January 2025, imposes strict requirements on information and communication technology resilience, incident reporting, and third-party risk management. Similarly, the Markets in Crypto-Assets Regulation (MiCA), fully applicable from December 2024, harmonises crypto-asset regulation across the EU, while the Financial Data Access (FIDA) regulation is advancing toward staged implementation later in the decade.

At the national level, regulators are embedding these EU-wide principles into local frameworks. For example:

**Latvia**
The Bank of Latvia's Guidelines for Monitoring, Managing and Mitigating the Risk of Financial Fraud (published May 19, 2025) formalise expectations for unified fraud-risk governance, complaint handling, and real-time reporting of digital fraud incidents to CERT.LV.

**Estonia**
The central bank established a Retail Payments Forum roundtable bringing together banks, telecom operators, the Information System Authority, CERT-EE, relevant ministries, the police, the E-identity solution provider, the Consumer Protection Authority, and financial supervisors

**Lithuania**
The new Fraud Prevention Guidelines (effective May 1, 2024) detail organisation, risk assessments, reimbursement practices, and customer resilience measures. The regulators have embraced what industry observers describe as a 'new normal' of stricter audits and supervisory reviews, with the central bank conducting frequent inspections across e-money and payment institutions.[14] This more rigorous stance is expected to enhance control maturity and drive greater transparency in fraud reporting across the market.

At the card-scheme level, global networks are aligning with regulators to strengthen ecosystem oversight. Visa's Acquirer Monitoring Program (VAMP) now consolidates fraud, dispute, and enumeration monitoring into a single performance metric, enabling Visa to identify acquirers or merchants with elevated risk profiles and enforce remediation more quickly.

[14] ThreatMark, The Baltics Under Pressure: RTP, Scams, and Smarter Fraud Defense, 2025: https://www.threatmark.com/baltics-under-pressure/

## Frameworks for close cooperation and coordination

The Baltic payments ecosystem is compact but sophisticated, built around close coordination between regulators, supervisors, industry associations, and innovation networks. The respective central banks – Eesti Pank, Latvijas Banka, and the Bank of Lithuania – act as the primary overseers of payment system stability, settlement infrastructure, and regulatory alignment. In Estonia, supervisory functions are carried out by Finantsinspektsioon (Financial Supervision Authority), while in Latvia and Lithuania the Central Banks carry dual monetary and supervisory mandates.

Industry associations and innovation platforms serve as key bridges between regulators and market participants:

**Latvia**
The Finance Latvia Association works closely with Latvijas Banka on payment modernisation and fraud risk guidelines, while the Latvia Fintech Forum – organised by Latvijas Banka, Latvian Investment and Development Agency (LIAA), and Riga's Investment Agency – facilitates dialogue among banks, fintechs, and government on licensing and innovation.

**Estonia**
The national Payment Forum, led by Eesti Pank, convenes banks, PSPs, and processors to align on SEPA standards, ISO 20022 adoption, and instant-payment readiness.

**Lithuania**
Communities such as Fintech Hub LT, ROCKIT, and Infobalt foster collaboration among startups, electronic money institutions (EMIs), and larger institutions under the Lithuanian Fintech Strategy 2023–2028, coordinated by the Ministry of Finance and supported by a multi-stakeholder Memorandum of Understanding.

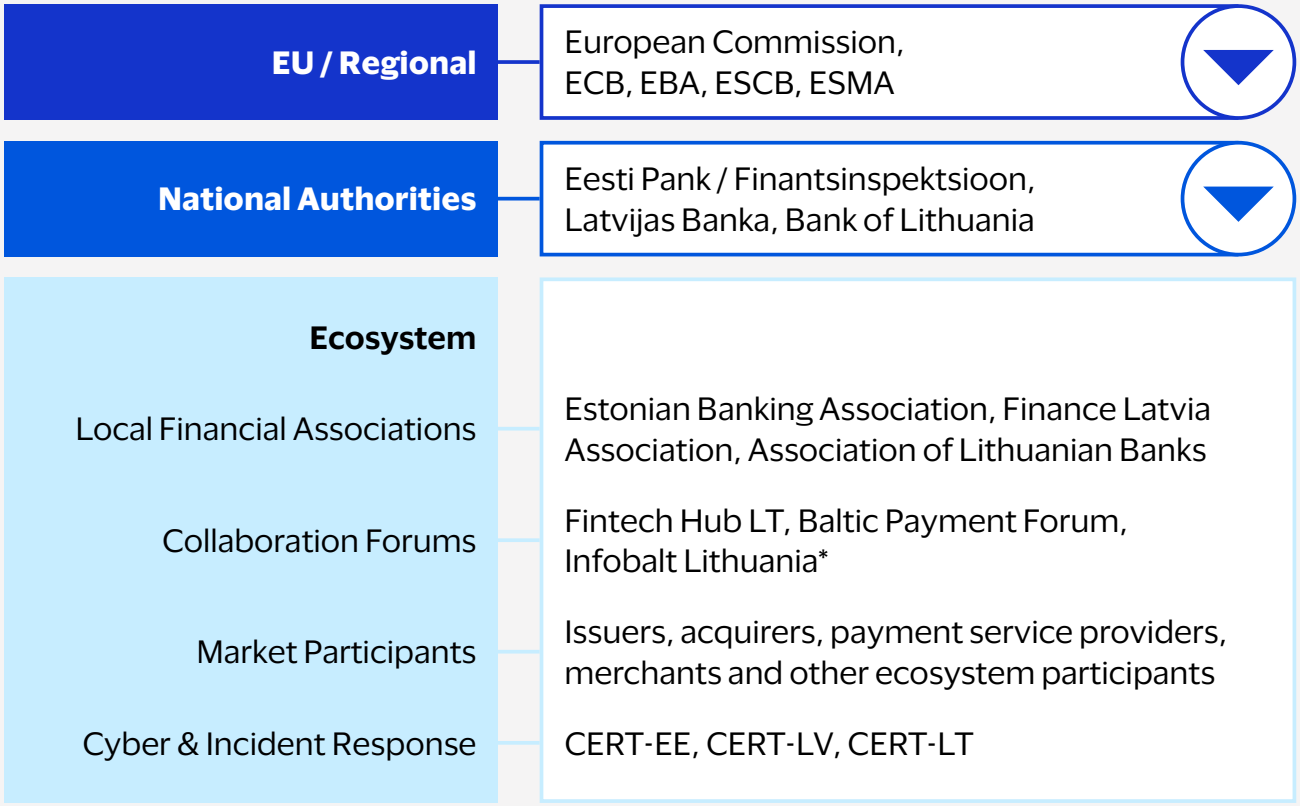
At the regional level, the Baltic Payment Forum acts as a cross-market coordination platform, bringing together payment and fraud-risk experts from the three countries alongside Nordic councils and card-scheme representatives. While primarily an industry event, it increasingly shapes strategies for fraud data-sharing and joint responses to cyber and financial threats.

Each Baltic country also operates a national Computer Emergency Response Team – CERT-EE, CERT.LV, and CERT-LT – which participate in the EU Computer Security Incident Response Team (CSIRT) Network under the Network and Information Security Directive 2 (NIS2) framework, serving as key cybersecurity coordinators. Financial institutions are encouraged (and in some cases required under national law) to report digital fraud incidents, phishing campaigns, and cyberattacks to their national CERT to enable real-time data exchange and coordinated alerts.

Inter-bank coordination is reinforced by central bank working groups and crisis management protocols, including rapid-response arrangements with telecom operators to block spoofed numbers and fraudulent SMS traffic – initiatives which are particularly active in Latvia and Lithuania. At the EU level, Baltic stakeholders participate in the European Payments Council's Fraud Information and Data Analytics (FRIDA) Task Force and the European Banking Authority's Expert Group on Payment Fraud, ensuring alignment with SEPA-wide standards and pan-European fraud prevention practices.

**This list in not exhaustive**

## REGULATORY/PAYMENTS LANDSCAPE IN THE BALTICS




*This list in not exhaustive

# The evolving fraud landscape – how the picture has shifted

## The story with payment cards

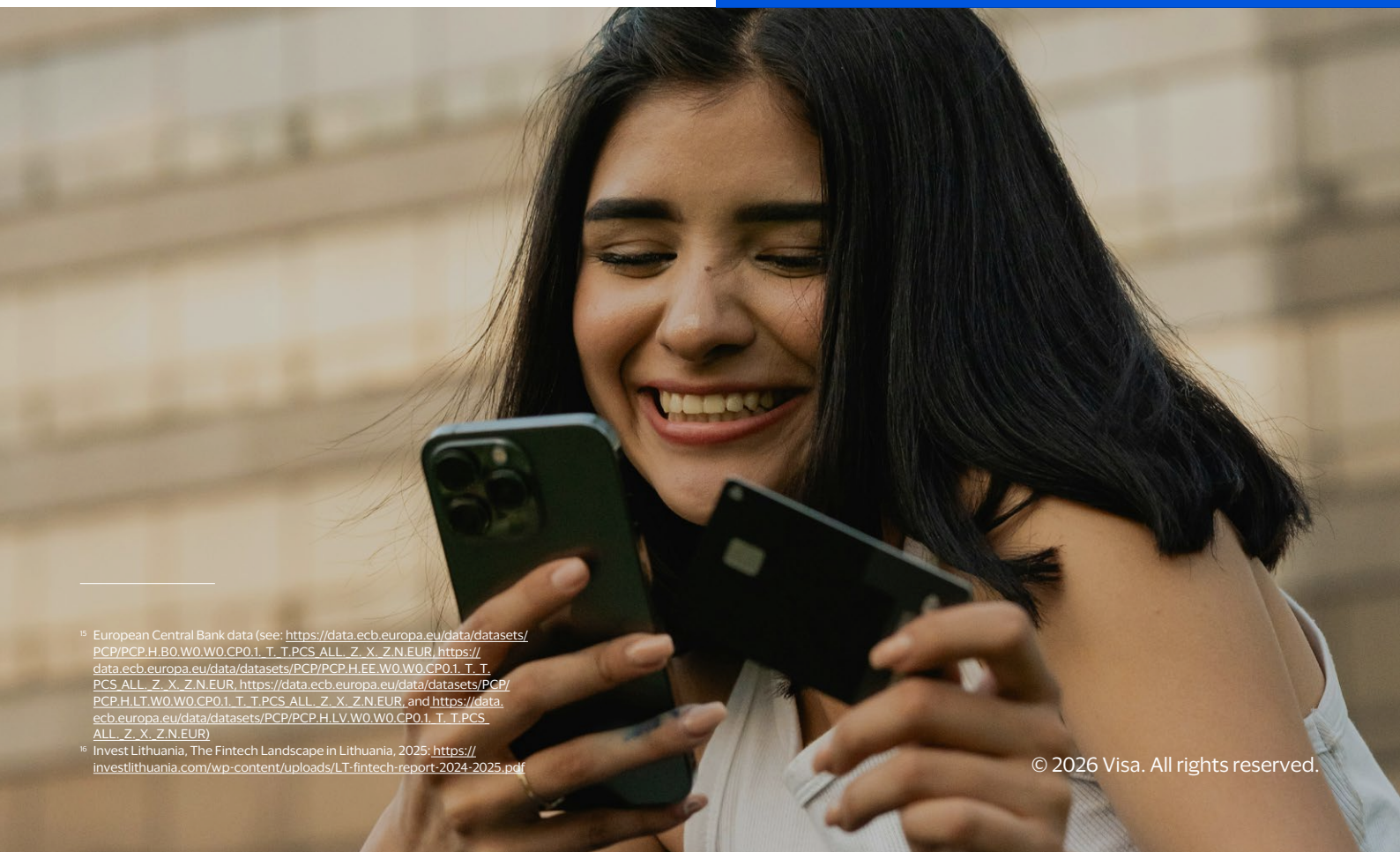
### ECB data – how the Baltics compares with the wider EU on card use

Between 2022 and 2024, the value of card payments across the euro area expanded at a compound annual growth rate (CAGR) of 12.7% to reach €3.7 trillion. The Baltic region outpaced this trajectory with 17.5% CAGR, although this aggregate figure conceals sharp national disparities: Lithuania was the primary growth engine, with payment values surging at 20.5% CAGR to reach €76.6 billion; by contrast, Estonia (8.3% CAGR) and Latvia (8.6% CAGR) grew more slowly than the EU benchmark.[15]

Lithuania's exceptional performance reflects several reinforcing factors: the country hosts the largest fintech ecosystem in the EU by number of licensed entities,[16] many of which issue cards to non-resident customers across Europe and channel cross-border e-commerce through Lithuanian-licensed platforms.

**Lithuania's card fraud-to-sales ratio jumped from 0.010 percent to 0.066 percent from H2 2022 to H1 2023,**

a near seven-fold increase, pushing losses from €3 million to €19.7 million



[15] European Central Bank data (see: https://data.ecb.europa.eu/data/datasets/PCP/PCP.H.B0.W0.W0.CP0.1._T._T.PCS_ALL._Z._X._Z.N.EUR, https://data.ecb.europa.eu/data/datasets/PCP/PCP.H.EE.W0.W0.CP0.1._T._T.PCS_ALL._Z._X._Z.N.EUR, https://data.ecb.europa.eu/data/datasets/PCP/PCP.H.LT.W0.W0.CP0.1._T._T.PCS_ALL._Z._X._Z.N.EUR, and https://data.ecb.europa.eu/data/datasets/PCP/PCP.H.LV.W0.W0.CP0.1._T._T.PCS_ALL._Z._X._Z.N.EUR)

[16] Invest Lithuania, The Fintech Landscape in Lithuania, 2025: https://investlithuania.com/wp-content/uploads/LT-fintech-report-2024-2025.pdf

## ECB data – how the Baltics compares with the wider EU on card fraud

Since 2022, EU fraud-to-sales (F2S) ratio (includes both card present and card not present (CNP)) has remained relatively stable at 0.031–0.035% – thanks in part to the implementation of Strong Customer Authentication (SCA) under PSD2 and the use of increasingly sophisticated fraud detection systems. Up until the second half of 2022, Baltic fraud rates remained well below the EU, with a blended F2S of just 0.011% – at around a third of the EU equivalent.[17]

Things shifted in the first half of 2023. Lithuania's F2S ratio spiked from 0.010% to 0.066% – a near seven-fold increase. This pushed the country's fraud rate to almost double the EU average, with absolute losses surging from €3.0 million in the second half of 2022 to €19.7 million in the first half of 2023. Estonia and Latvia experienced more modest increases. [17]

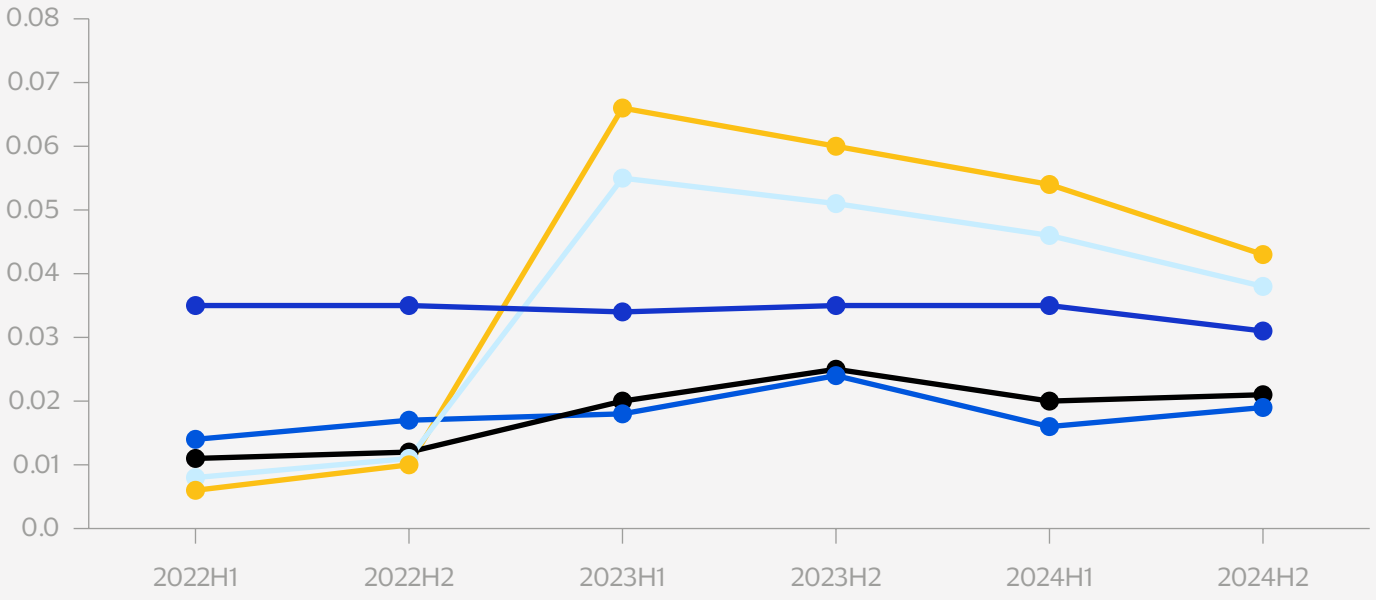
By the second half of 2024, Lithuania's F2S ratio had fallen to 0.043%, still more than triple the 2022 baseline and well above the EU average. Meanwhile, Estonia and Latvia stabilised near 0.020%, significantly below the EU average, but almost twice the level of the blended 2022 baseline. [17]

Lithuania's fraud surge coincides with several factors, including:

- Fintech-driven card issuance serving millions of non-resident customers expanded the attack surface for CNP fraud and account takeover
- Cross-border payment flows exposed institutions to fraud originating from jurisdictions with weaker controls
- Organised fraud networks intensified their activity, exploiting onboarding gaps and inconsistent use of multi-factor authentication (MFA)

It is worth noting that fraud reporting across the Baltics has historically faced certain challenges, with the potential that CNP fraud has been underreported.

### FRAUD TO SALES RATES, % – CARDS




ECB: Card payments, sent

[17] European Central Bank data (see: (https://data.ecb.europa.eu/data/datasets/PCP/PCP.H.B0.W0.W0.CP0.1._T._T.PCS_ALL._Z._X.F.N.EUR, https://data.ecb.europa.eu/data/datasets/PCP/PCP.H.EE.W0.W0.CP0.1._T._T.PCS_ALL._Z._X.F.N.EUR, https://data.ecb.europa.eu/data/datasets/PCP/PCP.H.LT.W0.W0.CP0.1._T._T.PCS_ALL._Z._X.F.N.EUR, and https://data.ecb.europa.eu/data/datasets/PCP/PCP.H.LV.W0.W0.CP0.1._T._T.PCS_ALL._Z._X.F.N.EUR)

## VisaNet data – the fraud performance among Baltic issuers

VisaNet data indicates a notable shift since early 2025: Estonia has experienced a sharp rise in F2S ratios (card present and CNP), reversing historical patterns. Intra-EU transactions now account for more than half of all Baltic card fraud, with criminal exploiting gaps in cross-border authentication and inconsistent enforcement of SCA. Domestic fraud remains stable, while inter-regional flows have moderated as issuers tightened cross-border monitoring.

Tokenization is proving decisive. Tokenized transactions now represent over one-third of total sales and exhibit significantly lower F2S ratios than legacy payment flows. The level of fraud in tokenized payment flows continues to decline year-on-year. However, over 95% of fraud losses remain concentrated in CNP transactions, which account for less than 40% of sales.

The weakest links are found in unsecured e-commerce (ECI 7–9) and mail order/telephone order (MOTO) channels.

### To address these vulnerabilities and sustain trust in digital payments, issuers and regulators should prioritise:

- Strengthening intra-EU authentication and monitoring, closing gaps in cross-border SCA enforcement
- Accelerating tokenization adoption in remote channels to reduce exposure to CNP fraud
- Remediating unsecured CNP and MOTO flows through adaptive 3-D Secure and dynamic risk-based authentication
- Deepening cross-issuer collaboration, including real-time intelligence sharing on compromised BINs and enumeration campaigns
- Complementing advanced measures with proven controls such as geo-blocking within banking apps to limit exposure to high-risk regions

## VisaNet data – the fraud performance among Baltic acquirers

Baltic acquirers have reduced F2S ratios by approximately seven basis points since the end of 2023, bringing rates broadly in line with the EU average as of mid-2025. Domestic transactions continue to show stable fraud levels with a gradual downward trend. Intra-EU payments remain the primary fraud driver, though recent improvements suggest that enhanced controls are beginning to take effect.

Tokenization adoption has accelerated, increasing by roughly ten percentage points over the past year and, as of mid-2025, representing about one-quarter of acquirer sales. However, non-tokenized CNP transactions still account for the majority of fraud losses. Notably, around a quarter of fraud losses sit in the "OTHER" ECI category, reflecting incomplete or missing e-commerce indicator reporting. This gap obscures authentication quality and hampers effective pattern analysis.

### To sustain progress and mitigate residual risks, acquirers should focus on:

- Accelerating tokenization across merchant portfolios, particularly in high-risk verticals
- Closing ECI reporting gaps through merchant education and system upgrades to improve fraud analytics
- Tightening controls on high-risk intra-EU corridors via enhanced due diligence and dynamic monitoring
- Expanding cross-acquirer intelligence sharing, including real-time alerts on compromised BINs and enumeration campaigns

## VisaNet data – how the Baltic CNP fraud performance varies by types of issuer

Using VisaNet data, we assessed the CNP fraud performance of three different types of issuers:

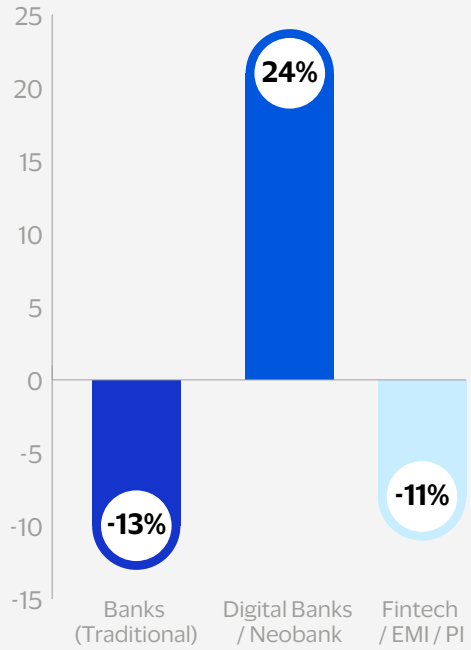
1. Traditional banks (defined as licensed institutions with physical branches)
2. Digital banks (defined as fully online entities that have a banking license or are in the process of obtaining a license)
3. Fintechs (defined as non-bank EMIs and payment institutions)

For each of these groups we analysed how the share of CNP volumes compares to the share of CNP fraud. So, for each one, we calculated the difference by subtracting its share of fraud from its share of volumes. The below chart illustrates these results:

- A negative value indicates disproportionately high fraud relative to transaction volumes (underperformance).
- A positive value indicates disproportionately low fraud relative to volumes (outperformance).

**BALTICS CARD NOT PRESENT FRAUD (ISSUER) – BANKS, DIGITAL BANKS, FINTECHS (Q2'24-Q2'25)**
**VisaNet Data**

### Issuer Categories: % share of volumes minus % share of fraud




Traditional banks and fintechs underperform, with their fraud exposure exceeding their transaction footprint. For traditional banks, elevated risk likely reflects legacy technology stacks, fragmented fraud detection systems, and slower adoption of real-time behavioural analytics. Fintechs show the greatest underperformance, especially in Estonia, where we assume that rapid customer onboarding and uneven MFA enforcement create vulnerabilities. By contrast, digital banks deliver the lowest F2S, likely supported by robust ID verification, seamless SCA integration, and unified data architectures enabling customer-level risk scoring.

For fraud leaders, these differential outcomes across issuer types offer actionable lessons. The superior performance of the digital banks demonstrates the potential of technology-led authentication and monitoring. By contrast, the sub-optimal performance of the fintechs demonstrates the risks of lagging regulatory alignment and cross-border exposure. Strengthening onboarding controls, enhancing screening for cross-border transactions, and strict SCA enforcement are immediate priorities for the fintech segment.

## VisaNet data – how the Baltics CNP Fraud performance compares by merchant category

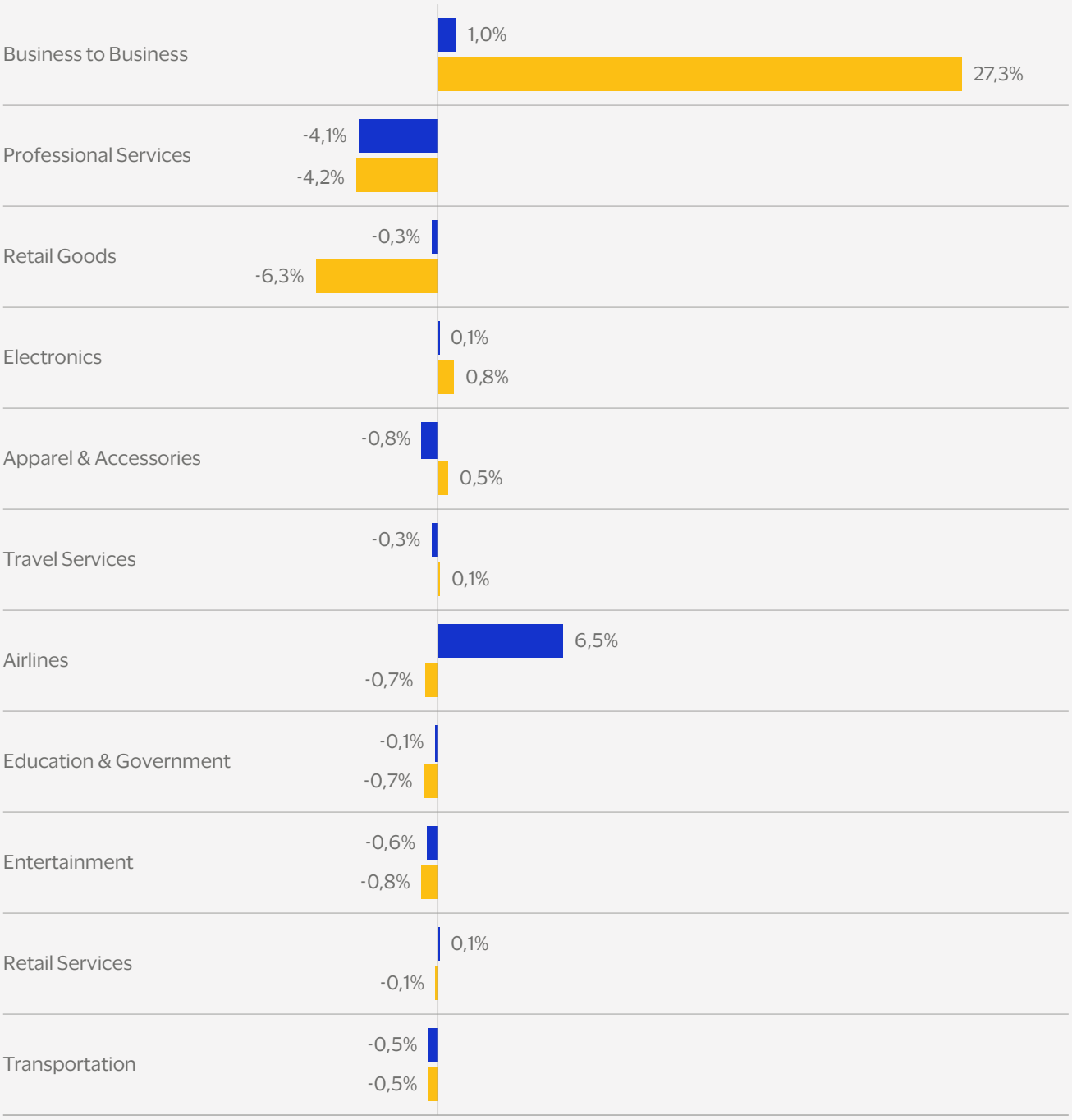
Overall, fraud has shifted from broad distribution to concentrated verticals. On the issuer side, B2B and professional services dominate losses, driven by the rapid growth of large-scale social media and digital advertising platforms. These merchants – characterised by card-on-file arrangements, subscription models, and limited per-transaction authentication – are ideal targets for testing stolen credentials and executing high-velocity fraud. As a result, they account for disproportionate losses.

For acquirers, digital-first sectors such as professional services, retail, and direct marketing carry elevated risks, with professional services alone responsible for the majority of acquirer losses. Digital-native financial platforms have become preferred cash-out channels for fraudsters – who use stolen cards to load funds onto prepaid or multi-currency accounts, then rapidly disperse proceeds through P2P transfers, alternative payment channels, and cross-border remittances. Instant onboarding, minimal friction, and real-time fund availability make these platforms attractive layering mechanisms for organised fraud rings.

Success now hinges on vertical-specific risk mapping and cross-chain intelligence to track fraud as it exploits low-friction digital commerce and real-time payment rails.

## BALTICS (ISSUER) — YEAR-OVER-YEAR PERCENTAGE-POINT CHANGE IN SHARE OF TOTAL CNP FRAUD AND SALES FOR TOP 10 MERCHANT CATEGORY GROUPS (2025 VS. 2024)

**VisaNet Data**



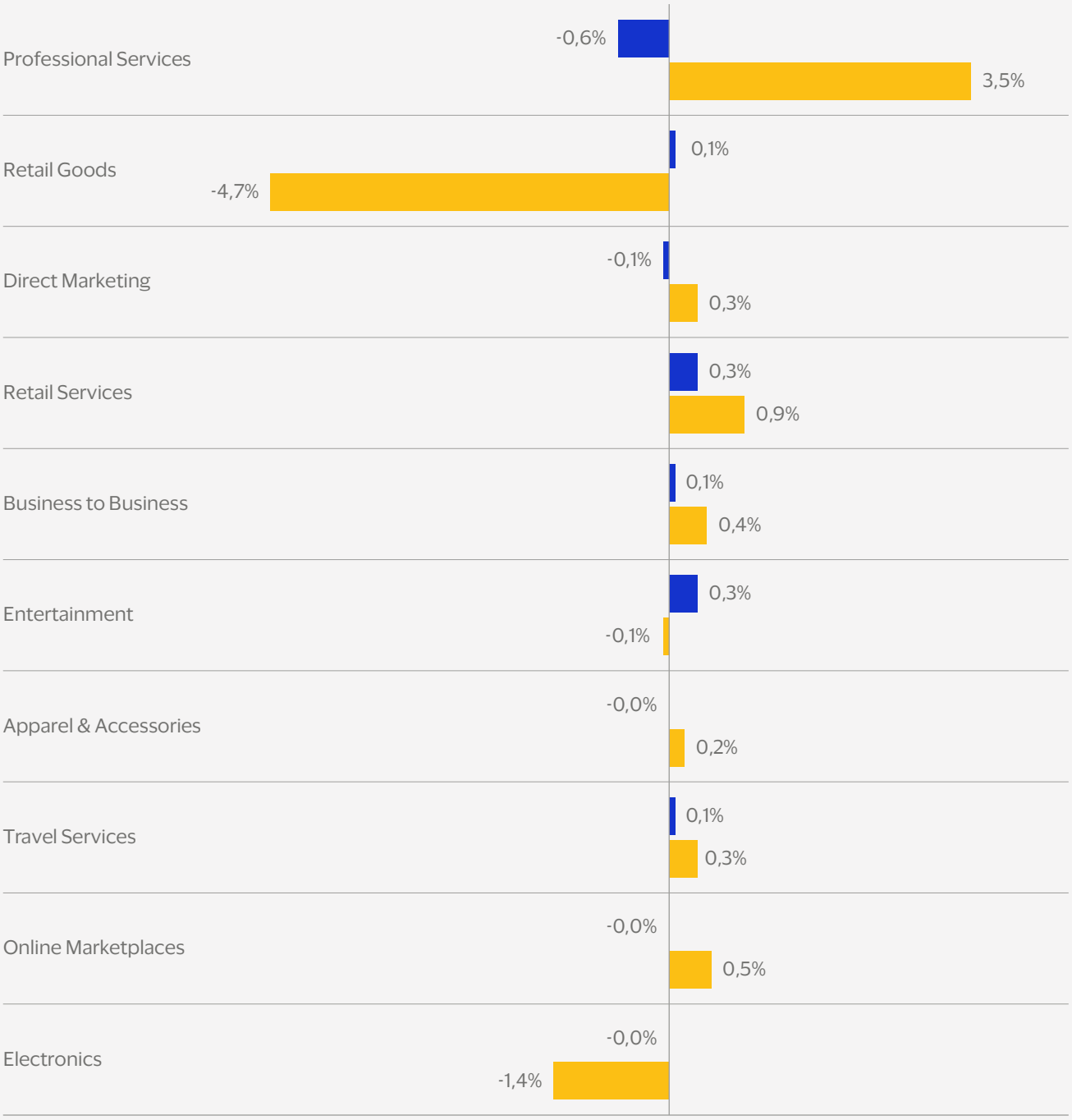

Legend

Change in % Share of Sales  Change in % Share of Fraud

Each bar shows the difference between 2025 and 2024 share of the Baltic total (in percentage points):
Positive value: The category's share increased in 2025 compared to 2024
Negative value: The category's share decreased in 2025 compared to 2024.
No absolute shares are displayed — only the change.

## BALTICS (ACQUIRER) — YEAR-OVER-YEAR PERCENTAGE-POINT CHANGE IN SHARE OF TOTAL CNP FRAUD AND SALES FOR TOP 10 MERCHANT CATEGORY GROUPS (2025 VS. 2024)

**VisaNet Data**




Legend

Change in % Share of Sales  Change in % Share of Fraud

Each bar shows the difference between 2025 and 2024 share of the Baltic total (in percentage points):
Positive value: The category's share increased in 2025 compared to 2024
Negative value: The category's share decreased in 2025 compared to 2024.
No absolute shares are displayed — only the change.

## The story with A2A/instant payments

### Rapid growth for A2A transactions, which are becoming deeply embedded in everyday payment behaviours

Europe is among the key regions driving A2A adoption, driven by SEPA infrastructure and PSD2. In 2024, the euro area processed around 150 billion non-cash payments worth more than €230 trillion (involving non-MFIs, i.e., end-user initiated non-cash payments), of which around 32 billion (21% of total) and €214 trillion (93% of total) were credit transfers.[18] This represents a 42% increase in volume and 43% in value since 2019.[19]

The Baltic states have emerged as pacesetters in the adoption of A2A payments. As of the second half of 2024, Latvia and Estonia had the highest share of credit transfers in the non-cash payments mix among all euro area countries – at 35.9% and 35.1%, respectively.[20]

Instant A2A transfers, measured as a share of credit transfer transactions processed by euro area retail payment systems, accounted for 4% of total value and 16% of total volume, with daily volumes surging by 72% between 2023 and 2024.[21] Industry projections suggest instant payments will rise to 30-40% of A2A volumes (processed by retail payment systems only) by the end of 2025 and approach 50% by 2026, spurred by the EU's Instant Payments Regulation (IPR).[22]

The Baltics lead Europe in instant payments adoption. Unlike markets dominated by standalone wallets, Baltic consumers heavily rely on direct bank integrations, making instant A2A the default for P2P transfers, bill payments, and e-commerce. Latvia was the first European country to deploy SCT Inst and has seen explosive growth: instant payment volumes surged from less than 12 million transactions (<€3 billion) in 2020 to around 60 million (>€20 billion) in 2024 – representing a compound annual growth rate of approximately 50% in volume and over 70% in value.[23] The growth trajectory remains strong,and similarly rapid increases are expected in Estonia and Lithuania as the instant payment infrastructure matures and regulatory momentum builds across the region.[24]

It's important to note that the adoption of instant payments across the Baltics has not just been rapid, it has also had distinct characteristics. Unlike markets dominated by standalone wallets, Baltic consumers rely on direct bank integrations, which has helped to make instant A2A the default for P2P transfers, bill payments, and e-commerce.

**42% & 43%**

increases in eurozone credit transfer volume and value, respectively, between 2019-2024

[18] Combined totals of the A2A performance figures provided by the European Central Bank for H1 and H2 2024: European Central Bank, Payments statistics: first half of 2024, 2025 (https://www.ecb.europa.eu/press/stats/paysec/html/ecb.pis2024h1-5263055ced.en.html); and European Central Bank, Payments statistics: second half of 2024, 2025 (https://www.ecb.europa.eu/press/stats/paysec/html/ecb.pis2024h2-5ada0087d2.en.html)

[19] European Central Bank, Payments statistics: 2019, 2020: https://www.ecb.europa.eu/press/stats/paysec/html/ecb.pis2019~71119b94d1.en.html

[20] European Central Bank, Payments statistics: second half of 2024, 2025: https://www.ecb.europa.eu/press/stats/paysec/html/ecb.pis2024h2~5ada0087d2.en.html

[21] Societe Generale, SEPA Instant Credit Transfers: Towards a new European standard? 2025: https://wholesale.banking.societegenerale.com/en/news-insights/all-news-insights/news-details/news/sepa-instant-credit-transfers-towards-a-new-european-standard/

[22] SBS, Are banks ready for the EU's instant payment revolution? 2025: https://sbs-software.com/insights/banks-eus-instant-payment-revolution/

[23] Latvijas Banka, Instant Payment Statistics, 2025: https://statdb.bank.lv/lb/Data/287

[24] CPG, European instant payment: what about this payment method in June 2023? 2023: https://www.cpg.de/en/european-instant-payment-what-about-this-payment-method-in-june-2023/

## How Baltic A2A fraud compares with EU norms

Credit transfer fraud rates in the Baltics remain higher than the European average, but the gap is narrowing.

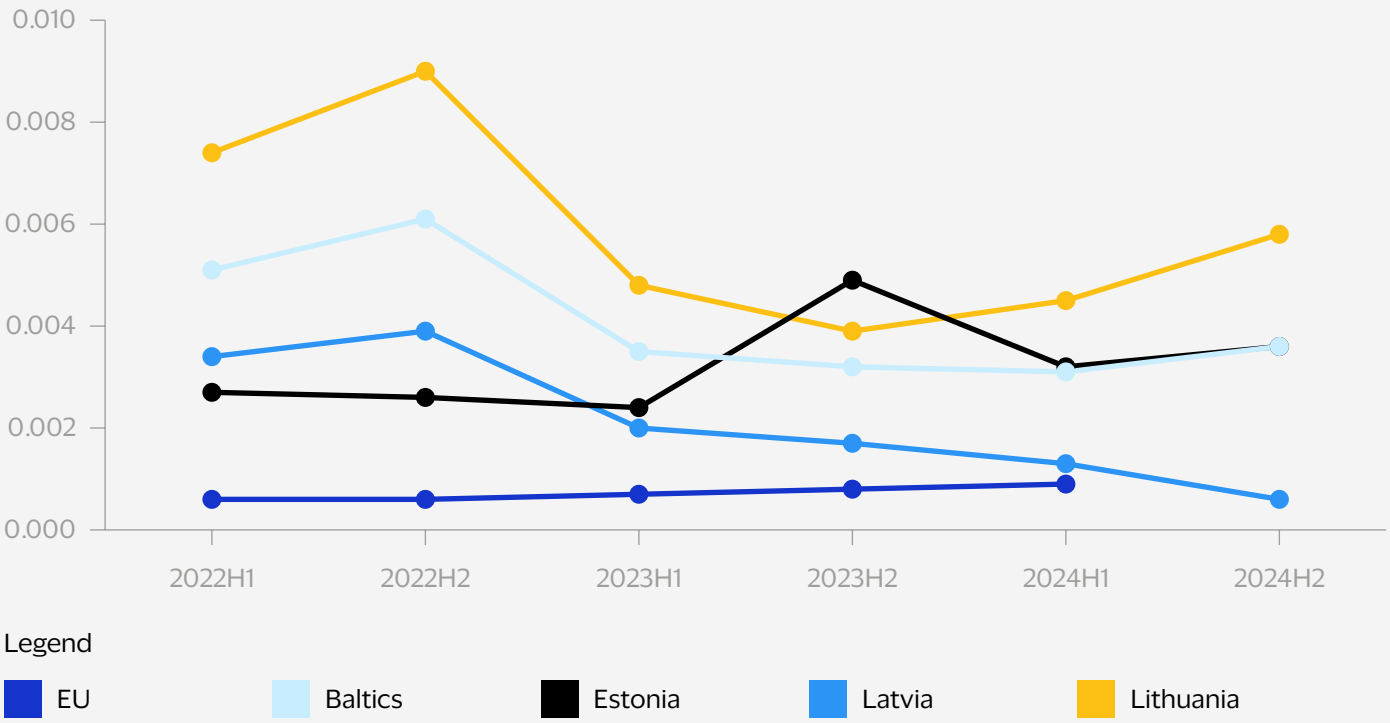
Across the EU, fraud losses on credit transfers have held steady for several years at roughly 0.001% of transaction value, equating to about €1 billion in fraudulent transfers in the first half of 2024 alone. By contrast, fraud intensity in the Baltics fell by nearly half, from 0.006% in the second half of 2022 to about 0.003% in the first half of 2024 – although there was an uptick in the second half of the year, to 0.004%.[25]

Among the Baltic countries, fraud levels are the lowest in Latvia. For the first half of 2024, the F2S ratio stood at 0.0013% before falling back to 0.0006% in the second half of the year, which is well below the EU average.

Lithuania reports the highest fraud rates in the region (0.0045% in the first half of 2024, rising to 0.0058% in the second half of the year) reflecting elevated risk exposure amid rapid payments growth and a large fintech ecosystem.[26]

In absolute terms, Baltic fraud losses are modest compared to Europe's total, but disproportionate: the Baltics account for only a small fraction of EU payment volume, yet an outsized share of EU fraud by value – roughly three-to-five times the volume share.[27]

### FRAUD TO SALES RATES, % – A2A




ECB: Total value of credit transfers all transactions, sent

[25] European Central Bank data (see: https://data.ecb.europa.eu/data/datasets/PCT/PCT.H.B0.W0.1._T._T.CTS_ALL._X._Z.N.EUR, https://data.ecb.europa.eu/data/datasets/PCT/PCT.H.EE.W0.1._T._T.CTS_ALL._X._Z.N.EUR, https://data.ecb.europa.eu/data/datasets/PCT/PCT.H.LT.W0.1._T._T.CTS_ALL._X._Z.N.EUR, https://data.ecb.europa.eu/data/datasets/PCT/PCT.H.LV.W0.1._T._T.CTS_ALL._X._Z.N.EUR, and https://data.ecb.europa.eu/data/datasets/PCT/PCT.H.B0.W0.1._T._T.CTS_ALL._X.F.N.EUR)

[26] European Central Bank data (see: https://data.ecb.europa.eu/data/datasets/PCT/PCT.H.EE.W0.1._T._T.CTS_ALL._X.F.N.EUR, https://data.ecb.europa.eu/data/datasets/PCT/PCT.H.LT.W0.1._T._T.CTS_ALL._X.F.N.EUR, https://data.ecb.europa.eu/data/datasets/PCT/PCT.H.LV.W0.1._T._T.CTS_ALL._X.F.N.EUR)

[27] European Central Bank data (see links in notes 24 and 25)

## Lessons to be drawn from the Nordic experience

Although the Baltics currently rely on direct bank integrations rather than standalone mobile wallets, the Nordic experience offers a glimpse of what may lie ahead.

In Sweden, Swish – used by over eight million people – has processed billions of real-time transfers, accelerating digital payments and embedding A2A into everyday commerce.[28] It's a similar story in Norway and Denmark, where Vipps and MobilePay have followed a similar trajectory, with these wallets now handling P2P, e-commerce, and point-of-sale transactions. However, their rapid growth has also exposed new vulnerabilities: in 2024 the Swedish Financial Supervisory Authority (Finansinspektionen) reported that payment fraud had reached its highest ever levels, with account transfers – including those via Swish – accounting for 85% of losses.[29]

As Baltic markets evolve, a homegrown wallet solution could emerge. This could bring added convenience and scale but also the need for robust fraud controls and enhanced network-level visibility.

85%

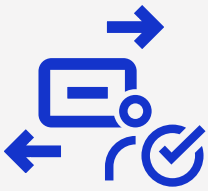
of Sweden's 2024 fraud losses came from account transfers, including Swish.

[28] FIxBE, The Swedish Fintech Ecosystem, 2024: https://www.fibe-berlin.com/en/newsroom/the-swedish-fintech-ecosystem.html
[29] Finansinspektionen, Fraud prevention in payment services, 2024: https://www.fi.se/en/published/reports/reports/2024/fraud-prevention-in-payment-services/

## The risk & fraud challenges of A2A/instant payments – and the regulatory response

The instant speed, irrevocability, and 24/7 availability of A2A transactions compress fraud detection windows to seconds, leaving no time for manual review. Funds are dispersed before red flags surface, and limited network visibility compounds the problem – sending banks rarely know recipient details unless both parties bank at the same institution, making risk assessment difficult, especially for APP fraud and money mule networks that move funds across banks and borders.

**24/7 availability of A2A transactions compress fraud detection windows to seconds**



**Funds are dispersed before red flags surface**

Given the risks, the regulators are stepping in on behalf of consumers. Back in October 2024, the UK implemented shared liability for APP fraud, requiring both sending and receiving banks to reimburse victims, and the EU is following suit. PSD3 and the PSR will shift liability for authorised fraud onto financial institutions (beyond PSD2's focus on unauthorised transactions). Under PSD3, PSPs must reimburse bank impersonation fraud victims, with burden of proof on the PSP to show customer fraud or gross negligence. The Instant Payments Regulation mandated VoP – which became active in October 2025 – requiring name-and-account matching before transfers to prevent misdirected payments and fraud. PSD3's broader provisions – including enhanced fraud data sharing, authentication standards, and APP compensation – are expected around 2026, which will place significant compliance and operational demands on payment players.

## The escalation of Authorised Push Payment (APP) fraud

APP fraud has become a particular issue with A2A transactions, with two main forms emerging:

- Malicious payee scams deceive victims into paying fraudsters for non-existent goods or services – including fake marketplaces, investment schemes, and romance scams.
- Malicious redirection scams involve the impersonation of banks, agencies, or contacts to divert funds – seen in business email compromise, invoice fraud, and impersonation attacks where fraudsters intercept legitimate payment instructions or claim accounts need 'securing'.

Both types of scam exploit psychology and trust. The finality of instant A2A transactions makes recovery nearly impossible once authorised. In the UK, APP fraud accounted for 41% of all payment fraud losses in the first half of 2025,[30] and similar trends are emerging across the Nordics and Baltics.[31]

## The implications for payment players

To compound the situation, shared liability and regulatory scrutiny drive higher costs, operational complexity, and continuous fraud prevention investments. Also, the reputational risk is acute – more than 90% of victims change their spending behaviour after experiencing fraud, with either reduced transaction frequency, less spend, or switching of bank provider.[32]

Mitigation is multi-layered. Real-time systems enabled by AI and machine learning (ML) analyse patterns, detect anomalies, and flag high-risk payments before completion. Network-level risk scoring and collaborative analytics identify mule accounts across institutions. Behavioural biometrics detect deviations from normal user patterns, flagging coercion in real time. Customer education counters social engineering.

Also, cross-sector collaboration – involving banks, regulators, law enforcement, and tech providers – is essential to outpace sophisticated fraud. The Nordic-Baltic region, with high digital adoption and interconnected systems, is a leader in these respects, but the evolving threat landscape demands relentless vigilance and innovation.

[30] UK Finance, Over £600 million stolen by fraudsters in first half of 2025, 2025: https://www.ukfinance.org.uk/news-and-insight/press-release/over-ps600-million-stolen-fraudsters-in-first-half-2025
[31] Visa Consulting & Analytics, Security and trust in Nordic payments, 2025: https://www.visa.co.uk/content/dam/VCOM/regional/ve/unitedkingdom/PDF/vca/uk-ndps-2024-security-and-trust-in-nordic-payments-vf.pdf
[32] Visa Acceptance Solutions, 2025 Global eCommerce Payments & Fraud Report, 2025: https://www.visaacceptance.com/en-us/insights/fraud-report.html

## Two dominant fraud channels across the Baltics

Fraud in the Baltics is now primarily concentrated in two channels: investment scams and vishing. Advanced social engineering, AI-powered impersonation, spoofed caller IDs, and real-time payment rails drive both.

And, although they have become the predominant risk across the region, there are important nuances – with each country showing unique patterns in composition, volume, and trends, shaped by their respective market structures and cross-border exposure:

### THE SITUATION IN LATVIA

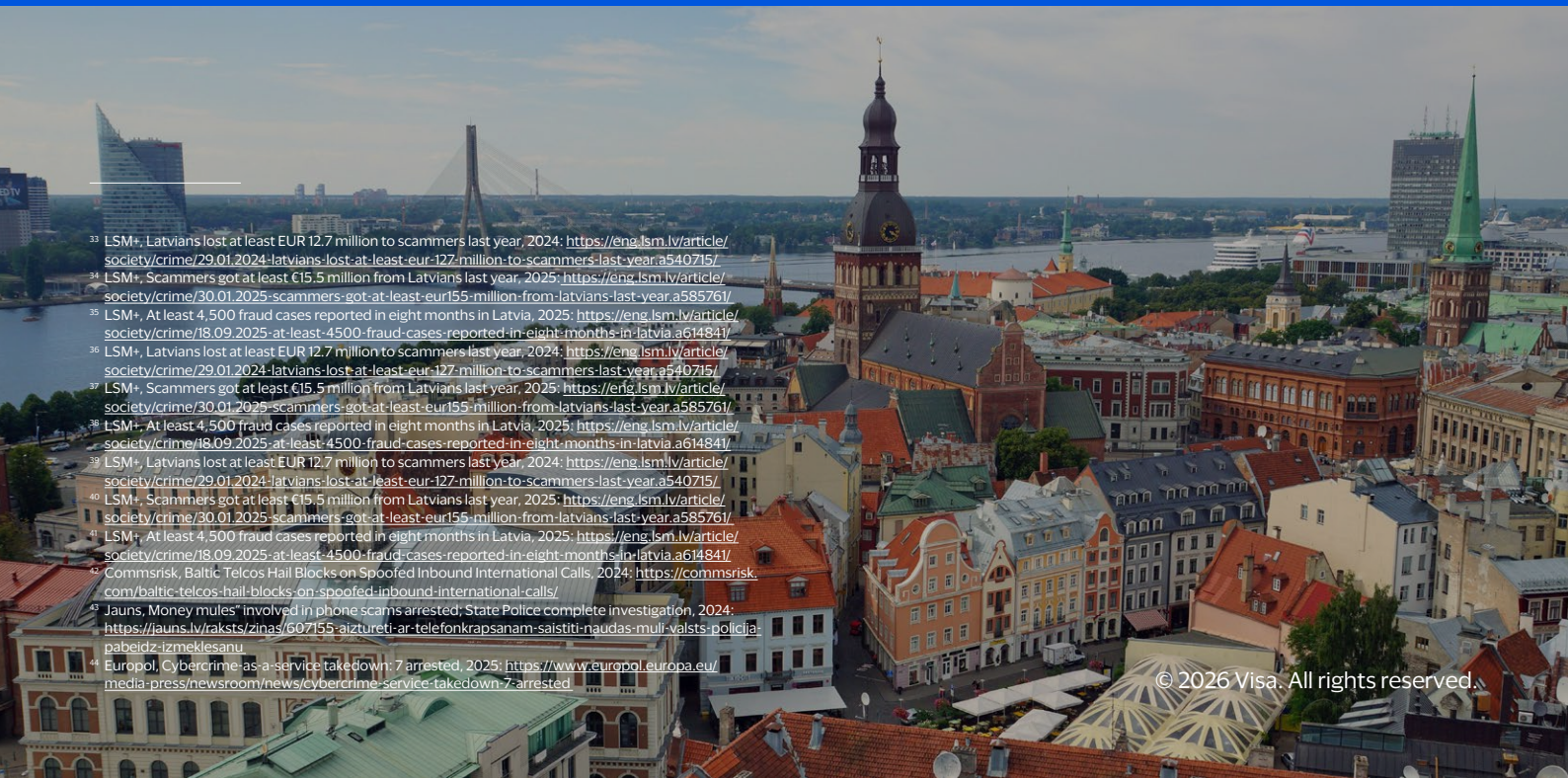
Fraud in Latvia has grown sharply in recent years but shows signs of stabilising in 2025. Losses rose from €12.7 million in 2023 to €15.5 million in 2024 (+22%), before moderating to €7.8 million in the first eight months of 2025. Case volumes followed a similar pattern: 7,795 in 2023, 9,025 in 2024, and 4,496 through to August 2025.[33, 34, 35]

The fraud mix is dominated by telephone scams (vishing) and investment fraud. In 2023, losses from both were nearly equal (about €5.6 million each). By 2025 year-to-date (8 months), vishing accounted for €4.3 million from 2,430 cases, while investment scams caused €3.0 million from 1,639 cases; other schemes added €0.6 million.[36, 37, 38]

Vishing schemes typically involve spoofed calls from fraudsters posing as banks, police, or government agencies, coercing victims to disclose credentials or transfer funds to 'safe' accounts.

Investment scams, lure victims with promises of high returns and direct them to fake trading platforms showing fabricated gains. Victims frequently make multiple transfers or take loans before realising they have been duped.

Preventive measures have scaled up: banks blocked €12.2 million in 2024 and €8.2 million in the first eight months of 2025, nearly matching actual losses.[39, 40, 41] Telecom operators now block a significant volume of spoofed international calls, intercepting tens of thousands of attempts monthly,[42] while law enforcement dismantled several foreign call centres and arrested over 100 money mules in 2024.[43] In October 2025, a major international operation coordinated by Europol and Eurojust led to the arrest of five Latvian nationals and the seizure of 1,200 SIM box devices and 40,000 active SIM cards. Investigators linked the criminal network to over 1,700 cyber fraud cases in Austria and 1,500 in Latvia, resulting in total losses of several million euros.[44]



[33] LSM+, Latvians lost at least EUR 12.7 million to scammers last year, 2024: https://eng.lsm.lv/article/society/crime/29.01.2024-latvians-lost-at-least-eur-127-million-to-scammers-last-year.a540715/
[34] LSM+, Scammers got at least €15.5 million from Latvians last year, 2025: https://eng.lsm.lv/article/society/crime/30.01.2025-scammers-got-at-least-eur155-million-from-latvians-last-year.a585761/
[35] LSM+, At least 4,500 fraud cases reported in eight months in Latvia, 2025: https://eng.lsm.lv/article/society/crime/18.09.2025-at-least-4500-fraud-cases-reported-in-eight-months-in-latvia.a614841/
[36] LSM+, Latvians lost at least EUR 12.7 million to scammers last year, 2024: https://eng.lsm.lv/article/society/crime/29.01.2024-latvians-lost-at-least-eur-127-million-to-scammers-last-year.a540715/
[37] LSM+, Scammers got at least €15.5 million from Latvians last year, 2025: https://eng.lsm.lv/article/society/crime/30.01.2025-scammers-got-at-least-eur155-million-from-latvians-last-year.a585761/
[38] LSM+, At least 4,500 fraud cases reported in eight months in Latvia, 2025: https://eng.lsm.lv/article/society/crime/18.09.2025-at-least-4500-fraud-cases-reported-in-eight-months-in-latvia.a614841/
[39] LSM+, Latvians lost at least EUR 12.7 million to scammers last year, 2024: https://eng.lsm.lv/article/society/crime/29.01.2024-latvians-lost-at-least-eur-127-million-to-scammers-last-year.a540715/
[40] LSM+, Scammers got at least €15.5 million from Latvians last year, 2025: https://eng.lsm.lv/article/society/crime/30.01.2025-scammers-got-at-least-eur155-million-from-latvians-last-year.a585761/
[41] LSM+, At least 4,500 fraud cases reported in eight months in Latvia, 2025: https://eng.lsm.lv/article/society/crime/18.09.2025-at-least-4500-fraud-cases-reported-in-eight-months-in-latvia.a614841/
[42] Commsrisk, Baltic Telcos Hail Blocks on Spoofed Inbound International Calls, 2024: https://commsrisk.com/baltic-telcos-hail-blocks-on-spoofed-inbound-international-calls/
[43] Jauns, Money mules" involved in phone scams arrested; State Police complete investigation, 2024: https://jauns.lv/raksts/zinas/607155-aizstureti-ar-telefonkrapsanam-saistiti-naudas-muli-valsts-policija-pabeidz-izmeklesanu
[44] Europol, Cybercrime-as-a-service takedown: 7 arrested, 2025: https://www.europol.europa.eu/media-press/newsroom/news/cybercrime-service-takedown-7-arrested

## THE SITUATION IN ESTONIA

In 2023, Estonians lost nearly €8 million to scams, with investment fraud accounting for €4.8 million and banking fraud for €2.3 million.[45] Towards the year-end, businesses faced a surge in invoice fraud, with individual losses reaching hundreds of thousands of euros, and similar patterns persisted in 2024, as banking fraud caused €2.3 million in losses and investment fraud exceeded €4 million.[46]
The fraud landscape remained dominated by phishing, vishing, and investment schemes, with criminals increasingly using Estonian-language calls and more sophisticated tactics.[47] In 2025, the trend shifted sharply: in the first eight months alone, banking fraud losses soared to €6.1 million, with both case volumes and average losses more than doubling – and June marked a record high, with over €2 million lost in a single month.[48]

Fraudsters increasingly impersonate banks, police, and government agencies – including the Health Insurance Fund– to trick victims into installing remote-access software (e.g., AnyDesk) and authorising transfers via Smart-ID (a digital identity solution for secure authentication and signing). Estonian-language scam calls have surged, with hundreds of thousands of euros stolen in recent months.

In May 2025 alone, 15 victims lost a combined €400,000 to Health Insurance Fund impersonation scams, including one case exceeding €200,000.[49] These calls typically claim the victim owes money for healthcare services or is entitled to a benefit, then attempt to obtain Smart-ID or Digi-ID PIN codes. Scammers often pose first as Health Insurance Fund employees, then as bank security officers, speaking native-level Estonian. Police believe the perpetrators operate from abroad and note active recruitment of Estonian-speaking call centre staff. Growing use of AI for Estonian-language voice generation raises concerns about future AI-driven scam calls. In a separate case, a company lost €1.7 million to fraudsters, underscoring the scale and impact of recent attacks.[50]

Estonia's legacy as a global hub for crypto-related financial crime also continues to shape its fraud landscape. As of mid-2021, nearly 55% of all virtual currency service providers worldwide were registered in Estonia, enabled by a liberal licensing regime. Many shell companies linked to money laundering and fraud have since shifted operations to neighbouring countries, but regulatory challenges remain.[51]

[45] The Baltic Times, Number of impactful cyber incidents in Estonia nearly doubled on year, 2025: https://www.baltictimes.com/number_of_impactful_cyber_incidents_in_estonia_nearly_doubled_on_year/
[46] The Baltic Times, Number of impactful cyber incidents in Estonia nearly doubled on year, 2025: https://www.baltictimes.com/number_of_impactful_cyber_incidents_in_estonia_nearly_doubled_on_year/
[47] Eesti Pank, The Estonian Payment Forum searched for ways of preventing payment fraud, 2025: https://www.eestipank.ee/en/press/estonian-payment-forum-searched-ways-preventing-payment-fraud-16012025
[48] ERR, Bank fraud on the rise in Estonia with €6.1 million stolen in 2025 so far, 2025: https://news.err.ee/1609826973/bank-fraud-on-the-rise-in-estonia-with-6-1-million-stolen-in-2025-so-far
[49] ERR, Estonian language phone scams becoming more common, 2025: https://news.err.ee/1609714302/estonian-language-phone-scams-becoming-more-common
[50] ERR, Estonian language phone scams becoming more common, 2025: https://news.err.ee/1609714302/estonian-language-phone-scams-becoming-more-common
[51] VSquare, Tales from the Crypto: How the Baltic states became the hub of money laundering, 2023: https://vsquare.org/tales-from-the-crypto-money-laundering-fraud-sanctions-estonia-lithuania-russia/

## THE SITUATION IN LITHUANIA

According to the Bank of Lithuania, fraudulent payments totalled €77.3 million in 2023 and increased to €89.7 million in 2024. In the first half of 2025 alone, €41.8 million was recorded, underscoring the persistent nature of fraud.[52]

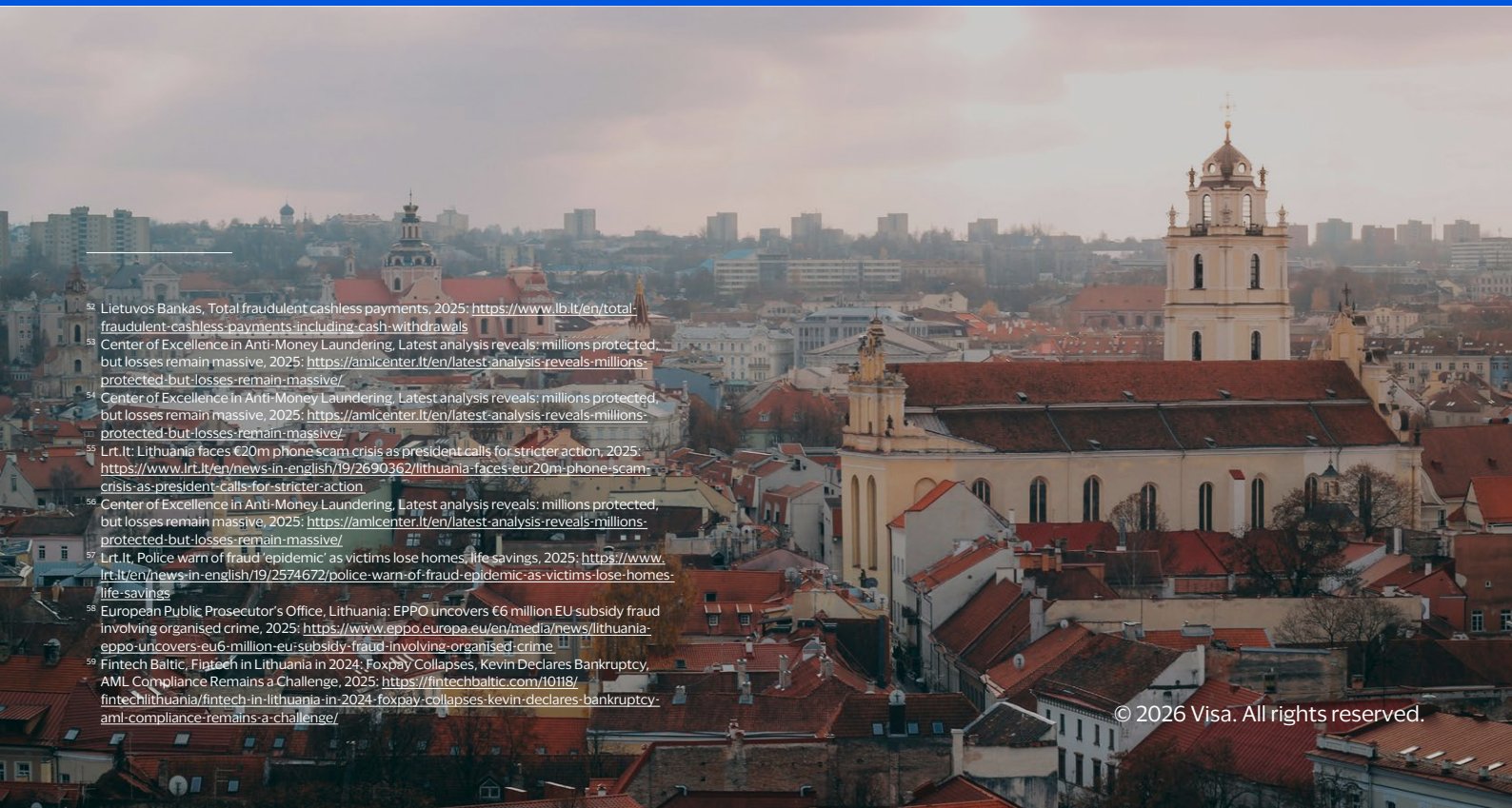
The country's Center of Excellence in Anti-Money Laundering reported record-high fraud in 2024, with €35 million targeted by criminals and over €20 million actually transferred – up from €11.8 million in 2022 and €12.3 million in 2023. Despite stronger prevention measures, only €2.6 million was recovered, leaving net losses at €17.3 million.[53]

Investment and phone (vishing) fraud together accounted for nearly €10 million in 2024 – almost half of all losses. Phone fraud surged, reaching €4.17 million in 2024 (up nearly 40% from €3 million in 2023).[54] In 2025, it accelerated dramatically, hitting €20 million by mid-year and prompting the president to call for specialised fraud investigation units.[55] Scammers increasingly use psychological manipulation, impersonating bank or law enforcement officials to pressure victims into transferring large sums.

Investment fraud also remained severe, with €5.57 million lost in 2024 – almost €800,000 more than in 2023. Phishing scams spiked as well, with 4,148 incidents and losses climbing from €1.6 million in 2023 to €3.42 million in 2024.[56]

Fraudsters in Lithuania employ sophisticated tactics, impersonating banks, police, and government agencies, and exploiting messaging apps and spoofed numbers. Victims are coerced into revealing credentials, installing remote-access software, or authorising transfers. Many fraud rings are highly professional and operate across borders, making recovery difficult – only about one-third of cases are solved.[57] Notable cases include a large-scale EU subsidy fraud, where an organised crime group misappropriated nearly €6 million from EU-funded projects,[58] and the Foxpay scandal in 2024, which involved the laundering of €17 and led to high-profile arrests.[59]

In response, authorities and financial institutions have strengthened prevention. The Bank of Lithuania introduced new guidelines in 2024 requiring real-time transaction monitoring and enhanced consumer education. Telecom providers now block suspicious calls and messages, and law enforcement has set up specialised units to investigate scams. Despite these efforts, the rapid evolution of fraud tactics and professional criminal networks continues to challenge prevention and enforcement.



[52] Lietuvos Bankas, Total fraudulent cashless payments, 2025: https://www.lb.lt/en/total-fraudulent-cashless-payments-including-cash-withdrawals
[53] Center of Excellence in Anti-Money Laundering, Latest analysis reveals: millions protected, but losses remain massive, 2025: https://amlcenter.lt/en/latest-analysis-reveals-millions-protected-but-losses-remain-massive/
[54] Center of Excellence in Anti-Money Laundering, Latest analysis reveals: millions protected, but losses remain massive, 2025: https://amlcenter.lt/en/latest-analysis-reveals-millions-protected-but-losses-remain-massive/
[55] Lrt.lt: Lithuania faces €20m phone scam crisis as president calls for stricter action, 2025: https://www.lrt.lt/en/news-in-english/19/2690362/lithuania-faces-eur20m-phone-scam-crisis-as-president-calls-for-stricter-action
[56] Center of Excellence in Anti-Money Laundering, Latest analysis reveals: millions protected, but losses remain massive, 2025: https://amlcenter.lt/en/latest-analysis-reveals-millions-protected-but-losses-remain-massive/
[57] Lrt.lt, Police warn of fraud 'epidemic' as victims lose homes, life savings, 2025: https://www.lrt.lt/en/news-in-english/19/2574672/police-warn-of-fraud-epidemic-as-victims-lose-homes-life-savings
[58] European Public Prosecutor's Office, Lithuania: EPPO uncovers €6 million EU subsidy fraud involving organised crime, 2025: https://www.eppo.europa.eu/en/media/news/lithuania-eppo-uncovers-eu6-million-eu-subsidy-fraud-involving-organised-crime
[59] Fintech Baltic, Fintech in Lithuania in 2024: Foxpay Collapses, Kevin Declares Bankruptcy, AML Compliance Remains a Challenge, 2025: https://fintechbaltic.com/10118/fintechlithuania/fintech-in-lithuania-in-2024-foxpay-collapses-kevin-declares-bankruptcy-aml-compliance-remains-a-challenge/

## Common tactics and modus operandi across the Baltics

Fraud schemes in Estonia, Latvia, and Lithuania share several characteristics:

### Language targeting

Fraudsters localise scripts and calls in Estonian, Latvian, Lithuanian, and Russian. Russian-language scams remain prevalent, especially in Latvia and Estonia, due to large Russian-speaking populations.

### Caller ID spoofing and telecom countermeasures

Scammers use technology to display local or institutional phone numbers, making calls appear legitimate. Lithuania and Latvia have implemented systems to block spoofed international calls, intercepting tens of thousands of fraudulent attempts each month.

### Multi-channel and multi-step attacks

Modern scams combine phone calls, SMS, email, and social media. Victims may receive phishing links or suspicious messages, followed by calls from individuals posing as bank or law enforcement officials, pressuring them to verify transactions or disclose sensitive information.

### Remote access and digital identity exploitation

Criminals instruct victims to install remote-access software (e.g., AnyDesk, TeamViewer) or to authorise payments via Smart-ID or Mobile-ID, enabling account takeover and unauthorised transfers. In Estonia, fraudsters increasingly use native-level Estonian in calls and target victims through the impersonation of Health Insurance Fund personnel.

### Psychological manipulation

Scammers employ urgent or emotional ruses – such as fake emergencies, police warnings, or promises of high investment returns – to coerce victims into transferring funds or revealing credentials.

### Money mule networks and cross-border laundering

Stolen funds are rapidly moved through networks of mule accounts, often crossing borders, which complicates recovery and law enforcement efforts. Professionalised fraud rings, sometimes operating from formal offices and trained abroad, are increasingly common.

### SIM box and cybercrime infrastructure

Large-scale operations use SIM boxes and thousands of SIM cards to automate scam calls. International law enforcement initiatives, such as the Europol and Eurojust-coordinated probe in Latvia, have led to arrests and the seizure of devices, disrupting major networks.

### Investment and vishing scams as dominant fraud types

Across all three countries, investment fraud and telephone scams (vishing) account for the largest share of losses. Investment scams lure victims with promises of high returns and direct them to fake trading platforms, while vishing schemes typically involve impersonation of banks, police, or government agencies.

### Rapid evolution and professionalisation

Fraud tactics continue to evolve, with increased use of AI for language and voice spoofing, and the emergence of highly organised, cross-border criminal networks.

## Victim profiles – who typically falls victim to fraud and why

Fraud risk in the Baltics mirrors EU trends, driven by age, education, and digital skills. Older adults incur the highest losses, while younger adults face more attempts. Only 56% of EU adults have basic digital skills, dropping to one-third among those 65+.[60] The gap between high- and low-education groups is nearly 46 percentage points, leaving less-educated individuals more exposed.[61]

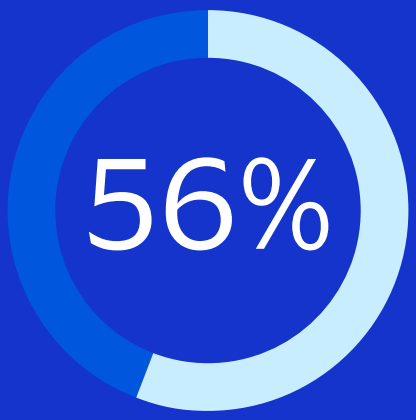
Phishing and social engineering have surged since 2023. Older and less digitally skilled individuals face a double risk: more likely to be deceived and less likely to report. In the Baltics, only 12% of victims reported fraud in 2024,[62] most blaming themselves – a mindset that hinders recovery and systemic learning.

Scams do not mainly target the very old or least educated. Javelin reports the highest prevalence among college-educated adults aged 25-44, driven by psychological pressure, not ignorance.[63] Success depends on urgency and confusion, not demographics. Even financial professionals – in a recent international survey, more than half have of finance professionals said they had experienced deepfake scamming, with 43% admitting they had fallen victim to such an attack[64] – proving that training alone is insufficient.

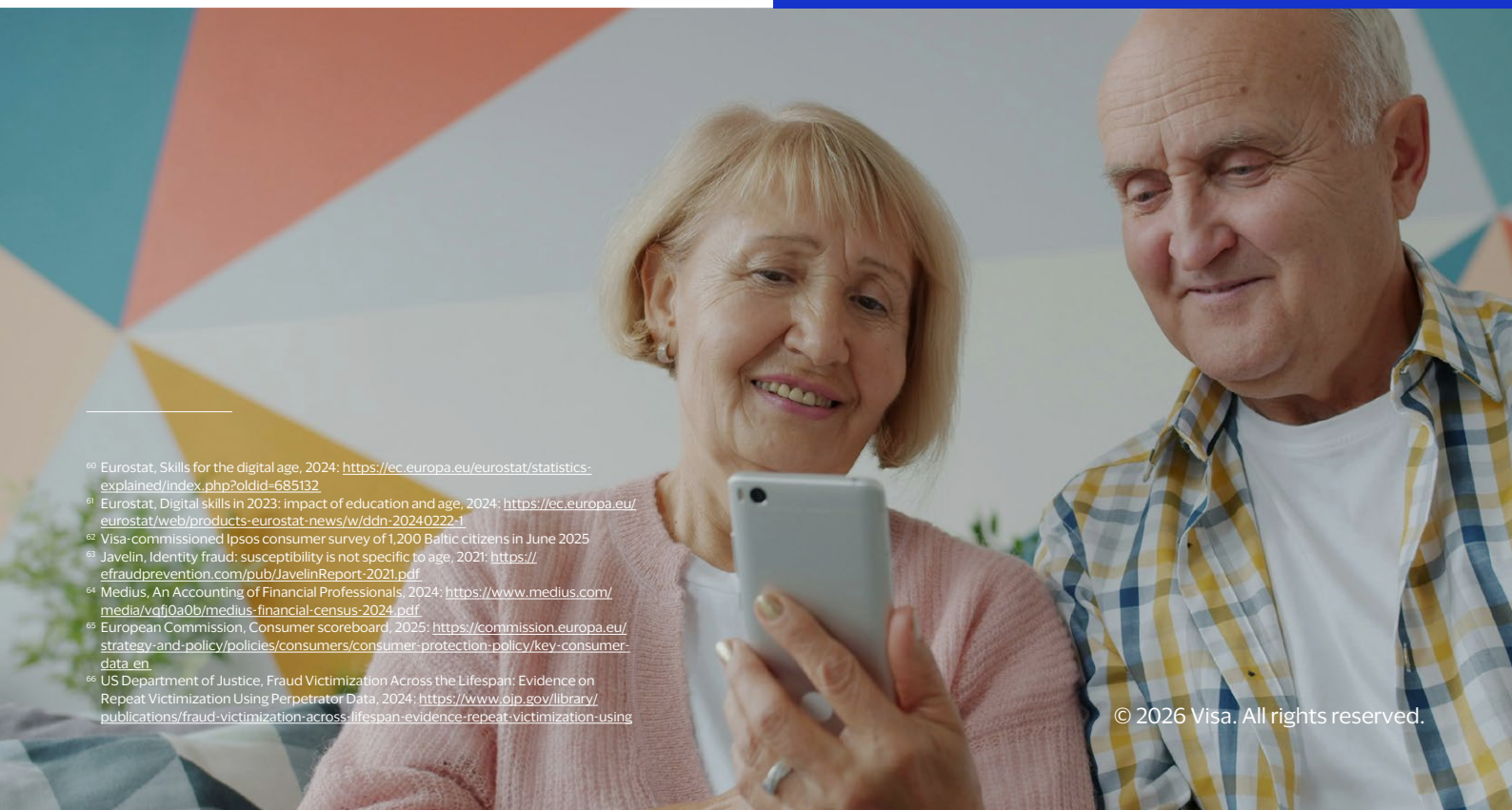
Scams are evolving with AI voice deepfakes and multi-step tactics using email, SMS, and calls. Many start with phishing links, followed by bank impersonation calls.

Multi-step scams exploit consumer confusion and inconsistent bank messaging. Legitimate texts resembling scams – like one-time-passcode (OTP) requests – heighten vulnerability. Phishing and APP scams dominate in the EU and Baltics, with nearly half of consumers targeted last year.[65] Under-reporting and reluctance to share behavioural data weaken detection efforts.

Repeat victimization is highest among isolated older adults without post-fraud support. Research suggests that those in their 70s and 80s are 9% more likely to be defrauded again than those in their 50s,[66] highlighting the need for immediate outreach and education.




of EU adults have basic digital skills



[60] Eurostat, Skills for the digital age, 2024: https://ec.europa.eu/eurostat/statistics-explained/index.php?oldid=685132
[61] Eurostat, Digital skills in 2023: impact of education and age, 2024: https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20240222-1
[62] Visa-commissioned Ipsos consumer survey of 1,200 Baltic citizens in June 2025
[63] Javelin, Identity fraud: susceptibility is not specific to age, 2021: https://efraudprevention.com/pub/JavelinReport-2021.pdf
[64] Medius, An Accounting of Financial Professionals, 2024: https://www.medius.com/media/vqfj0a0b/medius-financial-census-2024.pdf
[65] European Commission, Consumer scoreboard, 2025: https://commission.europa.eu/strategy-and-policy/policies/consumers/consumer-protection-policy/key-consumer-data_en
[66] US Department of Justice, Fraud Victimization Across the Lifespan: Evidence on Repeat Victimization Using Perpetrator Data, 2024: https://www.ojp.gov/library/publications/fraud-victimization-across-lifespan-evidence-repeat-victimization-using

# Executive perspectives and consumer insights

## What the practitioners tell us

VCA conducted a series of interviews with senior risk practitioners from leading banks, fintechs, payment processors, industry associations, and regulatory bodies across the Baltic region. These conversations included chief risk officers, heads of fraud, and experts from sector umbrella organisations. The interviews were held on an anonymous basis to encourage candid feedback and cross-sector perspectives.

The findings reveal that fraud prevention is universally prioritised, with institutions continuously adapting to new threats and regulatory demands. A2A fraud is now outpacing card fraud, driven by the instantaneous nature of these transactions and compounded by cross-border flows. Social engineering and investment scams dominate the landscape, while first-party fraud remains a persistent operational challenge. Institutions are migrating to advanced fraud tools and investing in unified data architecture, yet acknowledge gaps in real-time intelligence and cross-channel integration. AI-enabled threats and deepfake attacks are emerging, prompting layered defence strategies. Industry collaboration and intelligence sharing are valued as competitive differentiators – a clear indication that these network effects compound with participation. Regulatory uncertainty, especially around PSD3, continues to shape risk appetite and operational readiness. The sector recognises the importance of customer education and dark-web monitoring, but admits that banks and fintechs often remain one or two steps behind increasingly sophisticated fraudsters.

### Fraud prevention is a top priority

Fraud sits at the apex of every institution's agenda. Risk teams describe it as a mandate driven by external rules and internal imperatives: they staff teams around both card and A2A rails, map their risk frameworks accordingly, and ready themselves for the next tranche of scheme and regulatory demands.

> "We're preparing for VAMP; the first month under the new rules is coming up in October."

> "Cards and A2A are top of the list – the team is staffed accordingly and the risk framework is being enhanced continuously."

> "Fraud management is considered '10/10' priority – regulatory compliance, AML and fraud prevention are taken very seriously, with zero tolerance for fraud."

> "Fraud is a high priority topic in Estonia and across Europe; we are engaging more and more with all the market stakeholders."

Nevertheless, maintaining speed while adding controls is a constant tension, and the scale of losses underwrites the urgency. Respondents point to millions of euro per year disappearing from Baltic customers and note that the balance of security and convenience is never taken for granted.

## A2A fraud is surpassing card fraud

The rails that underpin the region's competitiveness have also become its largest attack surface. Practitioners observe that the volume and value of A2A fraud now exceed what they see on cards – and the interconnection of real-time flows means a scam can start in one jurisdiction and finish in another.

"Customers are losing more to A2A fraud year-over-year."

"The biggest challenge is tracing the full transactional fraud chain, which often starts outside the Baltics and ends in the region."

"It's not only private individuals; it's also individuals who are controlling corporate accounts, and then you see millions of euros being transferred."

"BIN calculator attacks and cash-outs happen in countries with weak EMV controls and then infect our rails."

Institutions have expanded headcount and rulesets for A2A specifically, tightened acceptance criteria, and built controls into push-payment rails that were originally designed for frictionless flow. The risk picture now encompasses cross-border cash-out corridors as much as domestic payments.

## Social engineering and investment scams dominate

Technical break-ins are receding; the human vector has become pre-eminent. Fraud leaders describe a landscape where persuasion and coercion outweigh brute-force breaches, and investment scams carry the biggest bite.

"Investment scams seem to be the only game in town."

"Even for me, as a payments expert, it's sometimes really difficult to distinguish what is real and what is not."

"We see a lot less of pure third-party fraud and account takeover; much more social engineering – the victim is coerced on the phone or via a website."

"AI provides the perfect tool to speak in local language, creating the illusion that leads customers to authorise payments or other transactions themselves."

"Social engineering at scale: less pure third-party account takeover – it's now becoming hybridised with ATO, making it hard to distinguish full takeover versus a manipulated victim."

Remediation must extend beyond rules and machine scores into customer education, deeper behavioural profiling, and cross-channel detection to catch a scripted phone call or a fake app as readily as a forged credential.

## First-party (friendly) fraud is a major pain point

The boundary between misuse and crime is blurred. Practitioners wrestle with definitions and the unintended consequences of scheme metrics that count wilful abuse as part of the fraud tally.

"Cardholder manipulation versus pure fraud – the ecosystem needs clearer definitions because today both count to the scheme's denominator under VAMP and distort the signal."

"75% of these frauds are friendly frauds and there's nothing friendly about it; if merchants or consumers want to dispute what they authorised, they should be criminalised, not rewarded."

"A merchant launching an illegitimate refund or a customer wilfully mistyping a beneficiary has a different risk profile than a traditional hijacked session."

Clear definitions matter because they determine how disputes are handled, how losses are recorded, and how cases are managed – ensuring that deliberate misuse is treated differently from external fraud.

## Migration to advanced fraud tools is underway

Legacy engines give way to specialist platforms and real-time analytics. The move is driven by the need to satisfy regulators and improve detection quality rather than to harvest direct cost savings.

"We run [Platform A] in real time and [Platform B] for retrospective analysis."

"Regulators must approve faster so we can evolve as fast as the fraudsters."

"We migrated from [Platform A] to [Platform B] after a careful review; the new version lets us score the merchant and portfolio, not just the card."

"We are testing behavioural biometrics and orchestration layers to improve detection and automate evidence for audits."

"The focus is on what banks can implement to help identify when activity on a bank account or in a wallet is not initiated by the customer, but by someone else. So, it goes more to the behavioural monitoring."

Institutions are focused on integrating new technologies that enable more granular scoring and real-time monitoring, with an eye to tying fraud alerts into customer relationship management (CRM) channels and supporting regulatory audits.

## Data architecture and unified risk scoring are gaps

The plumbing hasn't kept pace with the proliferation of channels. Siloes remain the norm and they hobble a unified risk view.

"Issuing, acquiring and A2A fraud live in separate silos."

"Our data runs faster than our governance."

"The card issuing system, the acquiring ledger and the retail banking risk monitor all sit on different data models; there's no single view to score a customer or merchant across channels."

"We are investing heavily in the data stack; you can't mitigate fraud without something akin to a data lake with a machine learning platform feeding all the silos."

The push now is toward a single customer or merchant score, cohort calibration, and data lakes that knit together card, account, and behavioural information into one picture.

## AI in fraud – a double-edged sword

AI is transforming fraud dynamics – empowering attackers while challenging defenders to innovate. Generative AI enables industrialised impersonation campaigns, forcing institutions to rethink authentication and detection strategies. At the same time, AI-driven prevention tools promise breakthroughs, but adoption comes with operational hurdles.

"We're testing our onboarding vendor via impersonation attacks and deepfake selfies."

"We're starting to see voice-cloned calls asking for a call-back – our fraud ops want to play back the call in slow motion to tease apart the clues."

"AI is not yet improving our fraud detection – but it is already improving the fraudster."

"The issue isn't false negatives anymore. It's too many false positives slowing review."

Simple rules cannot stop industrialised impersonation. The path forward requires layered defences – biometrics, behavioural analytics, and cryptography – combined with AI-driven detection tools tuned to minimise false positives without sacrificing speed.

## Regulatory uncertainty around PSD3 is a concern

Most interviewees are still working through PSD2 compliance and regard PSD3 as a distant, undefined destination. The unknowns dictate conservative policies and a readiness to adjust once the parameters are set.

> "We still manage cases over email; our process works but isn't scalable."

> "We're still working through PSD2 legacy rules, so PSD3 is a secondary focus."

> "The liability motivates self-regulation, and this is my hope – that this motivation actually improves the solutions at the end."

> "We know the reimbursement regime is going to change but we don't know how yet, so better to tighten the gate now."

> "Only when PSD3 is live do we know how big our Chief Risk Officer job becomes; today we calculate exposures like a best-guess and underwrite on the safe side."

Concerns include chargeback flows, extended liability to telcos or marketplaces, and evolving reimbursement thresholds.

## Industry collaboration is valued

No institution expects to prevail alone. The sector's defence relies on shared knowledge, joint forums, and cross-industry dialogue.

> "Fintech Hub Lithuania has proven effective in industry–regulator dialogue."

> "The Estonian Banking Association pulls together all the anti-financial crime leaders for workshops."

> "The association is building a fraud-intelligence sharing portal – it's overdue because fraudsters share information in real time but we share it in quarterly reports."

> "We are bringing all key stakeholders to the table, inviting relevant parties – banks, telecom providers, cybersecurity authorities, CERT teams, relevant ministries, the police, the digital ID solution provider, and consumer protection agencies. The goal is to create an overarching approach so that, as a nation, we have visibility into what is happening across different sectors and authorities."

Breaking down siloes at a systemic level is as important as breaking them within a bank. Real-time exchange across banks, telcos, platforms, and law enforcement is the glue that binds a resilient region.

## Cross-border fraud is a growing challenge

The geography that facilitates integration across Europe also attracts cross-border crime. Instant rails and light controls invite complex laundering chains.

"Criminals break into a foreign customer's account on Monday in Sweden, send money to Latvia on Tuesday and to an unregulated corridor on Wednesday – our challenge is to see it unfold across borders."

"The fraud starts in Western Europe or Asia but ends up in the Baltics because of lighter controls and large volumes of instant flows."

## The business case for investment is no longer clear cut

The calculus of investment in fraud prevention is evolving. Institutions recall a time when returns on such spending were highly favourable, but heightened regulatory scrutiny has shifted the balance.

"Cost saving and fraud management are not best friends."

"The main driver of current investment is also the compliance with regulatory requirements... that tops everything."

"Engineering salaries... we would expect five times the ROI. So that would be a happy medium for us and usually we would look at balancing that off. We started seeing victims' loss reimbursements coming to market, particularly the UK, and this changed the balance a lot... Previously it was like a 1:5, now we were suddenly talking about a 1:1 ratio... This is changing slowly back again... Perhaps there's one-to-three ratio... But we do expect PSD3 to change things quite a bit, which is why we're investing in vendors who are capable of providing us with a lot more of preventative and detective controls and therefore changing the ratio. So, it's likely that we'll swing to the 1:10 or 1:9 ratios approximately."

After a period of tighter margins, expectations are now improving as advanced capabilities are implemented. Still, compliance and customer experience remain dominant drivers.

## Customer education initiatives are assuming a higher profile

Customer education is increasingly recognised as a critical component of fraud prevention. Institutions are investing in awareness campaigns, targeted communications, and digital literacy programmes to help consumers recognise and avoid scams.

"We have launched regular fraud awareness campaigns to educate customers about the latest scam tactics."

"Our digital banking platform now includes interactive modules on safe payment practices."

"We plan to expand our outreach to older demographics who are less familiar with digital threats."

The importance of education is underscored by the prevalence of social engineering and investment scams. Practitioners note that informed customers are less likely to fall victim, and ongoing education is seen as essential to building long-term resilience.

## Achieving equilibrium has become a constant struggle

Institutions oscillate around an uneasy balance between blocking fraud and enabling business. Some believe they have achieved a workable state; others adjust dynamically.

"Too little control and we lose funds; too much and we lose customers."

"No transactions means no fraud, but that never works for merchants."

"Our group has stated it has low risk appetite – that's an overarching statement we must adhere to."

"Today with the current legal set-up... we are more on that balance of ensuring also the customer user experience is not too much interrupted."

"It's never stable; some months they [fraudsters] are going to be more aggressive, and it takes some time for us to adjust our controls."

"The thinking also has to change. Smooth payments have to be smooth indeed, but in today's world there will be some collateral damage from blocking, and that's fine. That's the new reality where we're living."

Risk appetite varies between institutions. Strong authentication enables a lighter touch; rising exposures prompt conservative shifts. Controls are often justified by compliance and reputational risk rather than ROI. The consensus is cautious progression – refine models, adjust controls, and await regulatory clarity.

## The dark web is a vital source of intelligence – but there are some stubborn gaps in coverage

Monitoring the dark web for emerging threats is a growing focus, but current intelligence collection remains fragmented. Institutions rely on vendor feeds, manual searches, and industry alerts to identify compromised data and fraud trends.

"We subscribe to several dark web monitoring services, but coverage is still patchy."

"Most intelligence is reactive; we often learn about breaches after the fact."

"There is a need for more proactive, real-time intelligence sharing across the sector."

Gaps persist in the ability to aggregate and act on dark web findings. Practitioners highlight the need for improved collaboration, automated tools, and integration with internal risk systems to close the intelligence loop and respond to emerging threats more quickly.

## A general sense of trepidation – with a few exceptions

Practitioners across the Baltics are clear-eyed about the future: fraud is evolving fast, and the region's readiness is uneven. Some institutions are investing heavily and feel cautiously optimistic; others admit they're underprepared, especially for tech-driven threats and regulatory shifts.

"We are always one or two steps behind the fraudsters."

"My opinion is that the region is not ready for the new emerging challenges, especially the technological challenges."

"Estonia, and much of the Baltics, is wildly underprepared for PSD3-style reimbursements and scheme dispute mechanics."

"We consider ourselves ready for upcoming changes... platform upgrades, AI and behavioural tooling, Baltic-wide collaboration."

"The biggest challenge is that fraudsters are more agile and better prepared than the industry, which is too robust and slow to react swiftly.'

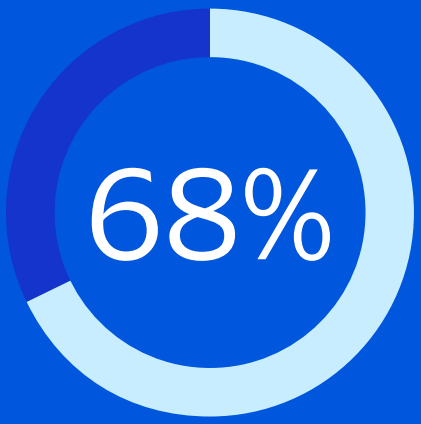
"Fraudsters invest a lot in market research... and into using AI. Most probably this is going to increase as well; I don't see that something will disappear from the table."

"We are facing a pandemic of fraud, with cases in the past nine months already surpassing the previous year – and the situation is worsening. Despite having a highly secure and seamless digital ID system, which we value, this convenience may be our greatest vulnerability. The fraud industry has become enormous, often outsourcing or procuring platforms from standard IT providers. It is crucial for law enforcement to monitor these fraud networks and raise awareness among IT companies to prevent indiscriminate distribution of code."

## It's not just the Baltics – similar themes are emerging internationally

The results of our interviews mirror the global picture, as demonstrated by a recent survey of 114 fraud executives conducted by Datos Insights:[67]

**96%** expect the use of AI by fraudsters to grow over the next five years



**68%** see enhanced information-sharing as the most promising detection trend

**76%** identify AI-based attack detection tools as the most effective fraud prevention method

**99%** consider the implementation of Agentic AI tools to monitor suspicious transactions within the next five years as 'very likely' or 'likely'


two-thirds rate the sophistication of fraudsters as equal to or greater than that of solution providers

**85%** anticipate moderate or significant increases in fraud-prevention budgets over the next five years – and they intend to direct those funds at AI and machine-learning, real-time transaction monitoring, identity verification and authentication solutions

[67] Datos Insights, Five Forces Disrupting Global Fraud Prevention by 2030, 2025: https://datos-insights.com/reports/five-forces-disrupting-global-fraud-prevention-by-2030/

## What the people tell us – new insights from original research

In June 2025, Ipsos ran a Visa-sponsored consumer survey among 1,200 people across the Baltics. This found that just over half of Baltic consumers – 51% – had encountered some form of fraud attempt in the previous year. Of those targeted, roughly 16% suffered a financial loss, with an average loss of about €105 per incident. Recovery of funds remains low – only 43% of fraud-related losses were eventually reimbursed to the victim, meaning the majority of fraud losses were never recovered.

Most fraud incidents occurred in a remote online shopping context. E-commerce was by far the most common setting for fraud attempts. Encouragingly, the majority of attempts did not lead to monetary loss – only about one-in-five targeted individuals ended up losing money, and in Latvia this figure was even lower (around 13% of those targeted).

When losses did occur, they tended to be modest – the most common amount lost was less than €20 (small purchases or fees). In terms of fraud methods, phishing emerged as the top threat, accounting for over half of reported fraud cases. The next most frequent schemes involved misleading subscription offers and fake product sales (e.g., non-delivery or false advertising).

The survey also exposed gaps in consumer awareness and perceptions of liability. Some 32% of respondents said that the consumer should be liable for money lost in a fraud incident – by far the most common answer, exceeding those who placed responsibility on banks, insurers, or platforms. At the same time, more than half of consumers were unaware that paying by card provides extra protections (such as chargeback rights) compared to A2A. This lack of awareness likely contributes to very low fraud reporting and dispute rates in the Baltics. Only 12% of fraud victims ever reported the issue or formally disputed the charges with their bank. The findings suggest that improving public awareness of fraud protections and liability could help increase reporting and recovery rates moving forward.

**51%**
of Baltic consumers experienced a fraud attempt in the past year

**12%**
of victims reported the incident

**60%**
of consumers are unaware that card payments offer more protection than A2A

# Prevent, detect and respond – tools for achieving equilibrium

## Using data and AI to combat payment fraud

As the Baltics accelerate towards real-time payments, fraudsters are evolving just as quickly. Financial institutions must respond with equally agile, intelligent, and layered defenses. Artificial Intelligence (AI) is at the heart of this transformation – but its true power is only unlocked when it's combined with consortium data, graph analytics, beneficiary risk scoring, and human-in-the-loop reviews.

Some two thirds (66%) of fraud executives at global financial institutions believe fraudsters are as sophisticated at least as sophisticated as solution providers. Almost all of them (96%) expect fraudsters to increase their use of AI to increase over the next five years. And three quarters (76%) identify AI-powered detection tools as the most promising approach to combating fraud.[68]

AI enables real-time fraud detection by analysing hundreds of transaction attributes in milliseconds. **Visa's Advanced Authorization (VAA)** processes over 500 variables per transaction and can scan up to 24 months of account history to intercept high-risk activity instantly. Building on this foundation, Visa's acquisition of **Featurespace** expands these capabilities even further. The integration of **Featurespace's ARIC™ Risk Hub** adds adaptive behavioural profiling, advanced analytics, and client-specific model customization – enabling Visa to enhance detection accuracy, reduce false positives, and faster decisioning across both card and A2A rails. Together, Visa's enterprise-scale network models and Featurespace's flexible, event-based platform provide broader coverage and a simplified client experience.

But no matter how sophisticated the platform that's being used, AI alone cannot address the full spectrum of fraud threats. Its impact peaks when integrated with:

- **Consortium data** – shared intelligence across institutions enhances pattern recognition and threat detection
- **Graph/mule analytics** – network-based analysis reveals hidden relationships and mule account activity
- **Beneficiary risk scoring** – evaluates the trustworthiness of recipients in push-payment flows
- **Human-in-the-loop reviews** – ensure nuanced decisions in edge cases and support continuous model refinement

To protect consumers and preserve trust, financial organisations must deploy a comprehensive fraud prevention strategy comprising:

- **Real-time transaction monitoring** – AI-driven systems flag anomalies instantly, reducing fraud losses and false positives
- **Robust authentication** – adaptive methods like biometric-ready, risk-based 3-D Secure (3DS) meet SCA standards while minimising friction
- **Behavioural intelligence** – machine learning models detect subtle shifts in user behaviour, often missed by rule-based systems
- **Customer education** – empowering users to recognise scams and act cautiously remains vital
- **Cross-institution collaboration** – shared threat intelligence improves ecosystem-wide resilience

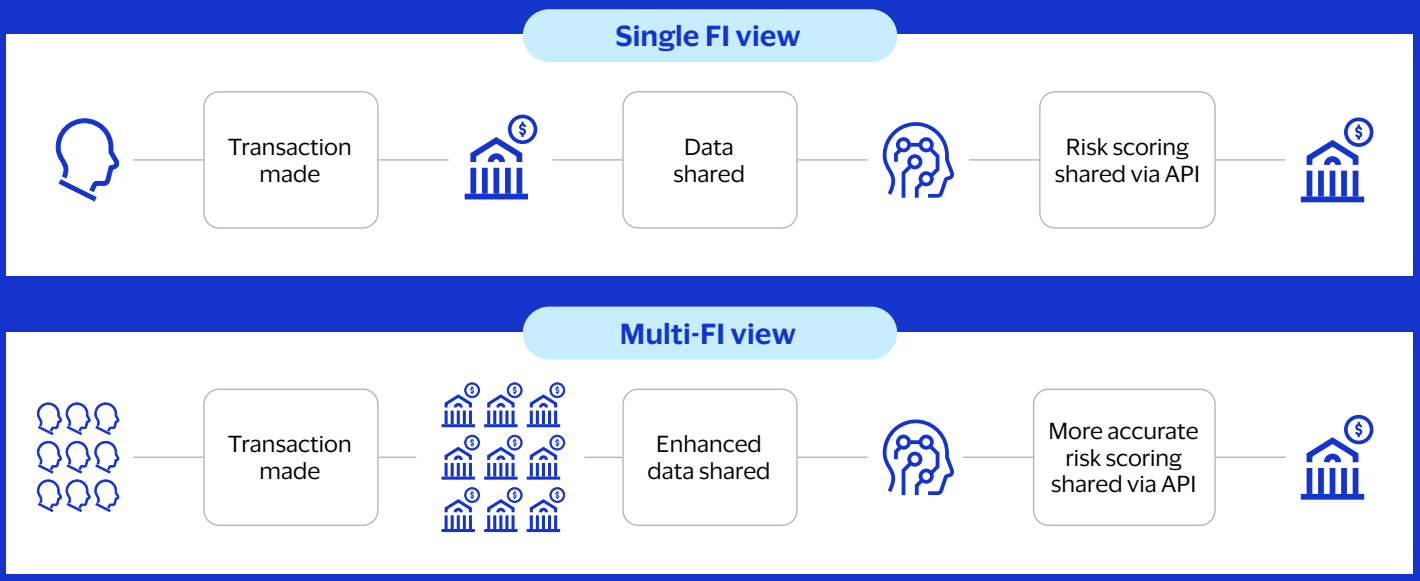
AI models trained on diverse, multi-bank data outperform isolated systems by enabling real-time risk scoring across payment rails, including cards and A2A transfers. They help detect mule networks before funds are moved, support instant payment compliance through standardised APIs and interoperable frameworks, and offer scalable infrastructure that balances speed, security, and cost. When combined with consortium data, graph analytics, beneficiary risk scoring, and human oversight, AI becomes a powerful tool in the fight against payments fraud. By uniting Visa's global AI network with Featurespace's adaptive technology, institutions gain expanded access, agility, and high-performance fraud analytics.

[68] Datos Insights, Five Forces Disrupting Global Fraud Prevention by 2030, 2025: https://datos-insights.com/reports/five-forces-disrupting-global-fraud-prevention-by-2030/

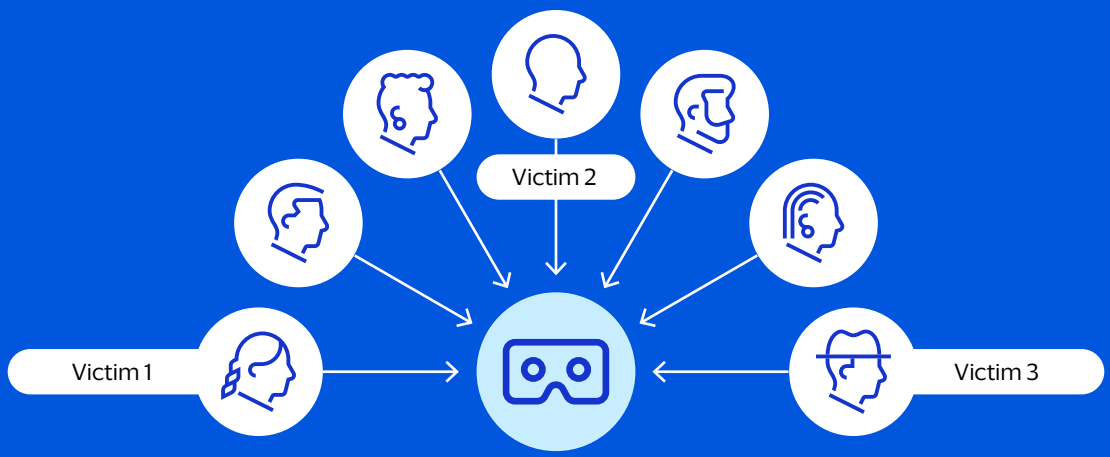
VISA

USING DATA AND AI TO COMBAT PAYMENTS FRAUD

# Single FI view versus multi-FI view




# Single FI visibility versus network-level visibiity




## Single FI view

**Victims bank is limited to their own data**

Cannot view scam account's activity

Scam account appears less risky than it is

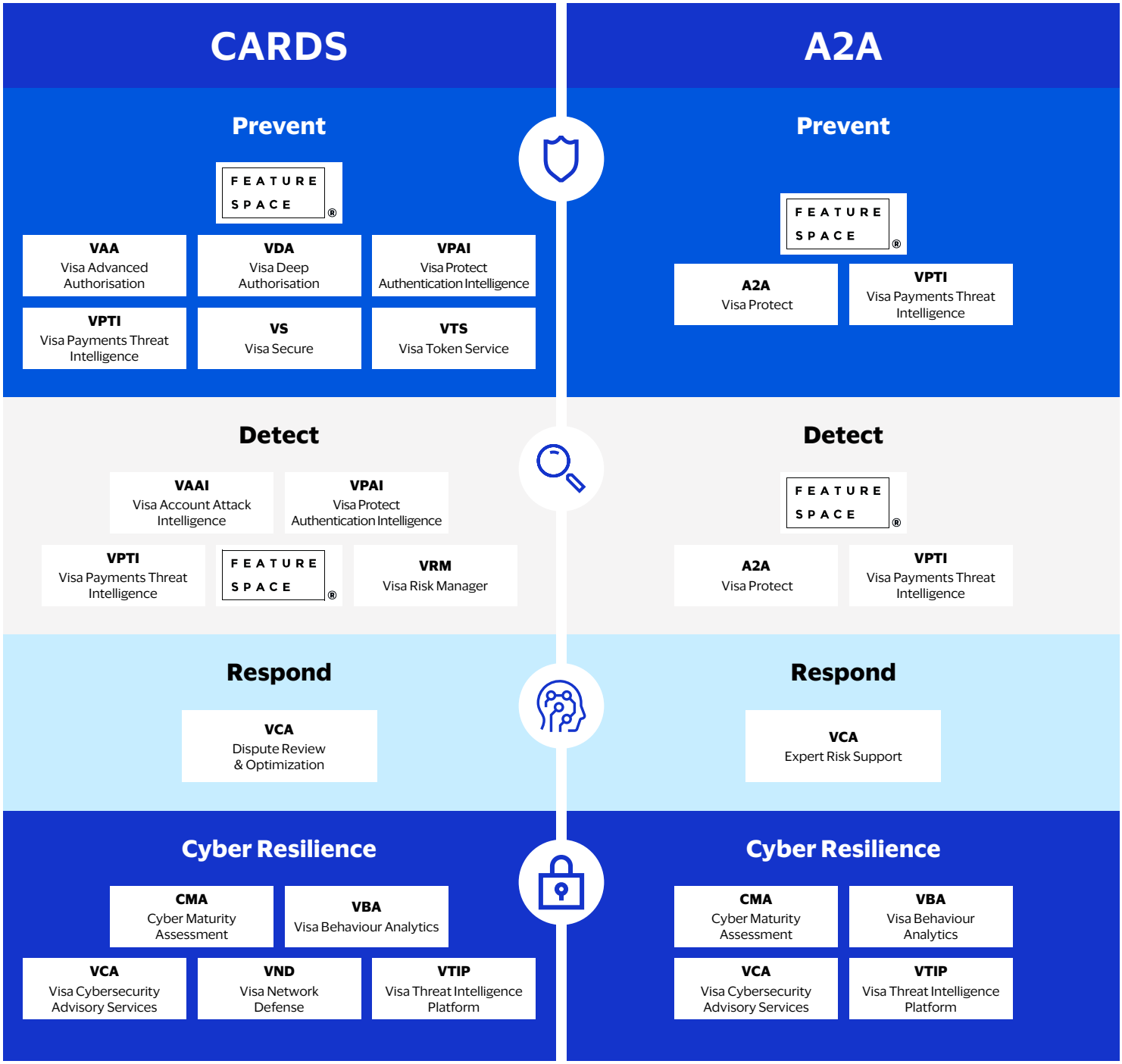
## Multi-FI view

**Multi-bank view provides enhanced risk perspective**

Full network activity shows that scammer has been receiving transactions from victims of other banks

Movement of funds (or layering) across network increases complexity of investigation

## OVERVIEW OF VISA RISK & FRAUD AND CYBERSECURITY SOLUTIONS (NON-EXHAUSTIVE)




Source: https://usa.visa.com/sites/visa-dps/our-solutions/dispute-management.html
https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.21586.html

The following pages go into more detail

This becomes a key enabler of the Prevent-Detect-Respond equilibrium:

### 1. The Prevent layer

Fraud prevention must be instant, layered, and low friction. Leading institutions now pair AI-based risk scoring, adaptive authentication (biometrics, RB-3DS), and tokenization with threat intelligence and mule-risk analytics to shrink attack surfaces and balance security with customer experience.

At Visa, prevention is driven by an integrated suite of solutions aligned with three pillars – security, speed, and savings – each reinforcing a different dimension of payment resilience across card and A2A rails.

Card fraud evolves in real time, forcing issuers to balance fraud losses against approval rates. At the authentication stage, **Visa Protect Authentication Intelligence (VPAI)** delivers superior fraud outcomes with low challenge rates for CNP transactions. It uses a supervised machine learning model that combines cross-channel data with EMV 3DS technology to generate a fraud propensity score, enabling seamless and secure cardholder authentication during online transactions. The score is shared with subscribing issuers via the **Visa Directory Server (DS)** in a message extension during the authentication request. Issuers then apply their own rules – typically based on score thresholds – to determine whether a transaction warrants step-up authentication.

At the authorisation stage, **Visa Advanced Authorization (VAA)** applies real-time AI scoring across hundreds of transaction variables, which can analyse up to 24 months of account history with multiple other data points, helping issuers intercept high-risk activity instantly. It analyses over 500 attributes per transaction in about one millisecond, strengthening both security and speed.

With the rise of instant and A2A payments, fraudsters exploit social engineering and APP scams. **Visa Protect for A2A and Card Payments** applies network-wide AI models to instant and A2A flows, spotting mule activity and social-engineering patterns in real time. The solution is further enhanced by Featurespace's adaptive behavioural analytics, integrated via the **ARIC™ Risk Hub**, which allows Visa to detect and block high-risk transactions prior to authorisation – delivering proactive prevention at network scale. It bridges speed, scale, and security across payment rails.

In e-commerce, identity and credential attacks dominate. **Risk-based 3DS** delivers adaptive, biometric-ready authentication that meets SCA standards and reduces false declines.

Credential theft remains a leading entry point for fraud. The **Visa Tokenization Services** replace sensitive card data with unique tokens, reducing exposure in digital commerce by more than 50%.[69] **Visa Deep Authorization (VDA)** adds contextual AI to CNP flows, improving precision without adding friction.

**Visa Cybersecurity Advisory Services** and **Visa Payments Threat Intelligence (VPTI)** help institutions strengthen defenses and anticipate emerging risks. VPTI's dark-web monitoring and early-warning alerts enable a faster response, while advisory services optimise fraud-control frameworks and compliance readiness.

Together, these solutions form Visa's preventive layer – a network of AI, authentication, and tokenization that protects transactions with security, speed, and efficiency across every rail.

[69] VisaNet, Europe, token vs. non-token card not present fraud, March 2022

## 2. The Detect layer

The detection layer provides continuous monitoring and early alerts, uses AI-driven scoring, and behavioural analytics to flag abnormal activity the instant it occurs. These tools integrate rule-based logic with machine learning, enabling institutions to identify new fraud patterns, adjust thresholds dynamically, and reduce both false positives and response times.

Issuers need continuous visibility and precise controls to stop emerging patterns without blunt declines or manual overload. **Visa Risk Manager (VRM)** gives issuers instant control 24/7 over transactions through configurable rules and behavioural alerts. It uses VAA's real-time insights and 80+ other transaction parameters to provide fraud rules creation capability. By combining automation and network intelligence, it cuts manual reviews by up to 40%,[70] strengthening both security and operational efficiency.

Cross-rail fraud demands unified protection. **Visa Protect Suite** leverages AI across cards, A2A, and wallets to uncover hidden patterns in real time. Its cross-rail visibility boosts detection accuracy while preserving seamless payment flows – delivering an extra 30% uplift in fraud detection when card and instant payments are analysed together, reinforcing security and speed at network scale.

Enumeration and card testing flood e-commerce, fuelling downstream fraud and depressing approval rates. **Visa Account Attack Intelligence (VAAI)** detects enumeration and credential-testing attempts in CNP traffic before they cause losses. Feeding alerts into issuer systems and programmes like **VAMP**, it builds hybrid resilience across the ecosystem. Enumeration attacks drive US$1.1 billion in annual global losses,[71] yet VAAI cuts false positives by 85% compared to other risk models,[72] and delivers decisions in just 20 milliseconds.[73]

New toolkits, mule services, and campaigns emerge before rules are tuned, extending incident dwell time. **Visa Payments Threat Intelligence (VPTI)** identifies emerging fraud risks from dark-web data and breach indicators, giving institutions the security insight to act before threats materialise, reducing high-cost incidents – boosting security and generating savings through avoided losses and faster investigations.

## 3. The Respond layer

When prevention and detection have done their part, response closes the loop, and focuses on minimising impact – resolving cases quickly, supporting victims, and restoring trust.

Fragmented chargeback handling drives write-offs, long cycle times, and poor customer experience. **Visa Dispute Management Services** centralises evidence gathering, representments, workflows, and scheme-rule compliance to resolve chargebacks efficiently on behalf of issuers/clients. This reduces average dispute resolution time from several weeks to as little as five days for participating issuers and acquirers, and improving win rates by over 20% through enhanced evidence automation and early resolution tools,[74] delivering measurable savings and greater customer satisfaction.

During attacks or emerging patterns, slow customer/ops outreach prolongs loss windows and increases call centre load. **Proactive Alerts & Case Management (VRM/DPS-integrated)**, tightly integrated with Visa Risk Manager and Visa DPS, enables near-real-time actions on scored events, reinforcing speed and security.

High-severity campaigns, account takeover bursts, or data compromises demand specialised case handling, communications, and cross-party coordination. **Expert Risk Support (Incident Response & Advisory)** provides 24/7 incident response with one of its KPIs of reduction of active fraud events within 24 hours of reporting, on-demand guidance from specialised fraud and cyber teams, and post-incident tuning aligned to scheme rules and regulatory expectations, enhancing security and long-term resilience.

[70] Visa, Pay.UK fraud detection pilot achieves overwhelming success with help from Visa, 2024: https://corporate.visa.com/content/dam/VCOM/corporate/products/documents/visa-protect-for-a2a-payments-pay.uk-case-study.pdf

[71] Enumeration Fraud Loss from VAAI FY23 (from https://investor.visa.com/news/news-details/2024/Visa-Announces-Generative-AI-Powered-Fraud-Solution-to-Combat-Account-Attacks/default.aspx)

[72] 2024 U.S. Visa Account Attack Intelligence Score Model Documentation (from https://investor.visa.com/news/news-details/2024/Visa-Announces-Generative-AI-Powered-Fraud-Solution-to-Combat-Account-Attacks/default.aspx)

[73] In adopting AI models VAAI can evaluate up to 182 risk attributes in a millisecond to derive a two-digit risk score predicting the likelihood of enumeration attack (from https://investor.visa.com/news/news-details/2024/Visa-Announces-Generative-AI-Powered-Fraud-Solution-to-Combat-Account-Attacks/default.aspx)

[74] Based on all transactions disputed via the Allocation and Collaboration flows within VROL as of February 2023 (from https://usa.visa.com/content/dam/VCOM/regional/na/us/Solutions/pps/visa-dispute-management-service-one-pager.pdf)

## The importance of cyber resilience

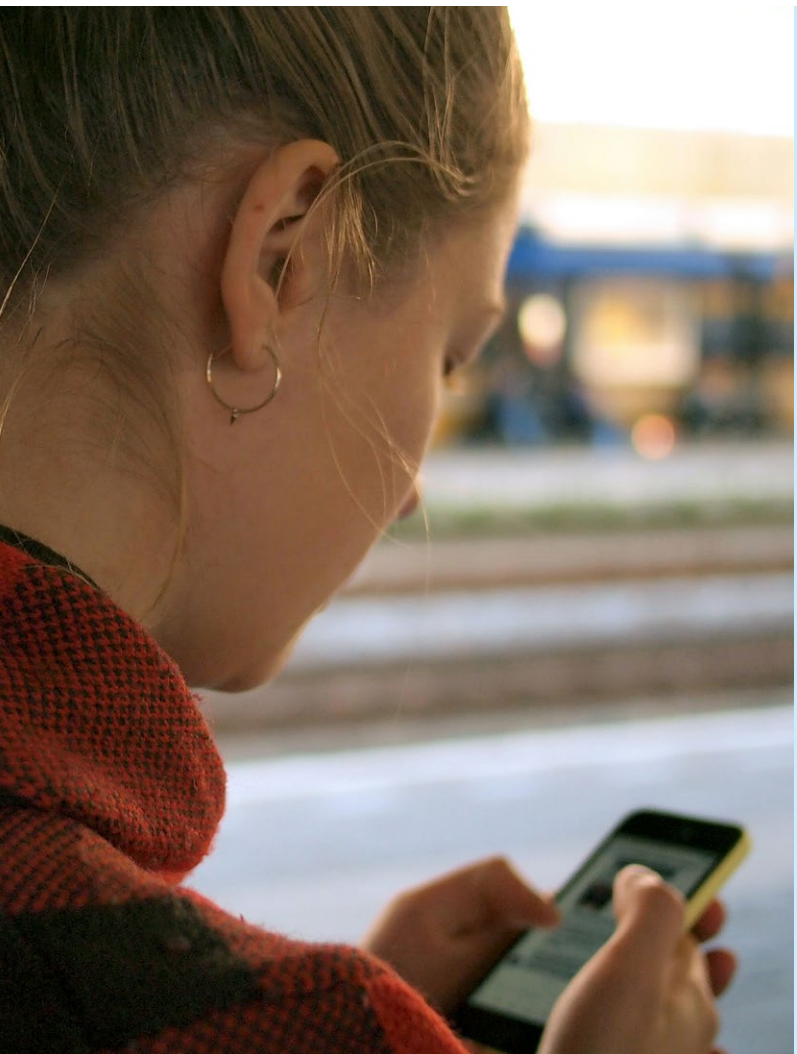
True resilience requires the ability to withstand and recover from broader cyber threats. Visa's cybersecurity solutions extend protection beyond the transaction layer, safeguarding payment ecosystems end-to-end, and build resilience for the future.

**Visa Network Defense (VND)** reinforces this perimeter by using AI and network telemetry to detect and disrupt coordinated cyberattacks across VisaNet and its connected partners, containing threats before they impact operations or payment flows.

The **Visa Threat Intelligence Platform (VTIP)** delivers continuous monitoring of threat indicators from open, deep, and dark web sources, transforming raw intelligence into actionable alerts before risks materialise. **Visa Behaviour Analytics** complements this by profiling normal user and system activity, flagging deviations that may signal credential compromise such as account takeover (ATO), insider threats, or malware infiltration – enabling faster, more accurate containment.

Through partnerships such as **Expel Managed Detection and Response (MDR)**, Visa provides 24/7 human-in-the-loop incident assessment, automated enrichment, and proactive remediation across diverse tech stacks. **Cyber Maturity Assessments** benchmark organisations across key domains, including governance, human, and physical security, to identify gaps against industry standards and prioritise actions to strengthen the overall cyber posture.

Together, these capabilities strengthen security by identifying and neutralising threats early, maintain speed by reducing dwell time from detection to remediation, and deliver savings through avoided breaches and operational efficiency – building the cyber resilience needed to sustain trust in an era of constant digital risk. These cybersecurity capabilities extend beyond payment transactions, supporting issuers, acquirers, merchants, and fintechs alike in safeguarding their businesses from evolving digital threats.



Lets take a look at a recent case study on how cyber resilience reduced phishing attacks

# Case study: How Featurespace helped Eika reduce phishing losses by 90%

Based in Norway, Eika is a strategic alliance of 46 local banks. Its core mission is to help small, community-based banks offer modern and efficient banking services. In 2022 and 2023, Eika faced significant financial losses due to phishing attacks and turned to Featurespace to help address the challenge.

Acquired by Visa in 2024, Featurespace is a global leader in adaptive fraud detection, using advanced machine learning to analyse every transaction- identifying both typical and suspicious behaviour to detect emerging fraud tactics in real time.

**90%**
reduction in phishing losses in 2024

**5 weeks**
to implement the Featurespace Payment Fraud Prevention Solution

## The challenge

Before partnering with Featurespace, Eika's team relied heavily on manual checks and email notifications to block user authentication and recall payments. This reactive approach required around-the-clock vigilance and placed unsustainable strain on staff and systems. Eika was facing three key challenges.

Rising fraud rates: Banks across Norway were seeing a sharp rise in fraud attempts, especially phishing scams targeting elderly customers.

Sophisticated fraud patterns: Increasingly complex and evolving attack methods were outpacing the capabilities of Eika's existing fraud prevention systems.

Manual review limitations: The growing volume of transactions made manual reviews time-intensive, error-prone, and operationally unsustainable.

## The results

Following implementation in December 2023, Eika saw an immediate and sustained reduction in fraud. By 2024, phishing losses had dropped by nearly 90% compared to the previous year.

Featurespace has provided Eika with a comprehensive, real-time customer view and the ability to automate previously manual processes. This has enabled the team to help stop fraudulent activity before payments are initiated, while also improving operational efficiency across the organisation.

> "In 2022 and 2023, we were struggling with a lot of phishing and huge losses. With the Featurespace solution fully integrated at the end of 2023, I'm pleased to share that we've reduced our phishing losses by almost 90% in 2024.
>
> **Jon Hagen**
> Chief IT Architect, Eika

Source: Featurespace. Eika, making Norway a safer place to transact

# Future-proofing – achieving sustainable equilibrium

## What is on the horizon?

The forces of change are set to escalate and accelerate. So, the fraud management response must be equally agile and dynamic. And, looking ahead, we envisage that six forces will define fraud prevention:

### 1. The AI arms race – defence and offence will both scale

Enterprise AI spend is accelerating sharply. IDC projects US$1.3 trillion in global AI spending by 2029, with a ~32% YoY growth trajectory from 2025 to 2029.[75] Meanwhile, while Gartner estimates GenAI spending alone will reach ~US$644 billion in 2025 as AI becomes embedded across devices, software and services.[76] At the same time, fraud actors are weaponising AI to accelerate social-engineering (voice cloning, deepfakes) and to industrialise CNP enumeration and account testing at scale. Visa's Payment Ecosystem Risk & Control team estimates ~US$1.1 billion in follow-on fraud annually from enumeration schemes, with attack volumes up ~22% in the second half of 2024.[77] And, as we explore in this paper, nearly all fraud leaders expect the use of AI among fraudsters to increase.

Baltic institutions are already encountering AI's double edge. Several report 'native language' scam calls generated synthetically, while others test biometric systems against deepfake impersonation. As one risk officer summarised: "AI is not yet improving our fraud detection – but it is already improving the fraudster." Many banks still rely on early-generation detection tools poorly integrated with CRM data, leaving gaps across card, A2A, and customer communication channels.

### 2. A2A keeps rising – bigger surface, bigger tickets

Instant and A2A payments will keep compounding: Capgemini's World Payments Report 2025 forecasts instant payments to reach 22% of all global non-cash volumes by 2028, with A2A offsetting 15–25% of card volume growth in some markets, and the European Payments Initiative (EPI) further accelerating A2A adoption.[78] Juniper Research sees global A2A value will reach ~US$195 trillion by 2030 on real-time rails and recurring models.[79]

Critically for risk teams, APP/credit-transfer fraud incidents tend to have higher value per case than card disputes, a pattern the EBA/ECB and European industry have flagged (transfers are fewer but larger, hence the EU's VoP push). In the UK, APP investment-scam losses rose to £144.4m in 2024 even as cases fell,[80] illustrating the 'fewer, bigger' profile relative to CNP fraud. Baltic financial institutions confirm that investment and impersonation scams now dominate, with losses accelerating through 2025. Detection windows have shrunk from minutes to seconds – which is too short for manual review – making AI-driven scoring and device intelligence essential.

Global A2A payment value is projected to hit roughly US$195 trillion by 2030.

[75] IDC, Agentic AI to Dominate IT Budget Expansion Over Next Five Years, Exceeding 26% of Worldwide IT Spending, and $1.3 Trillion in 2029, According to IDC, 2025: https://my.idc.com/getdoc.jsp?containerId=prUS53765225
[76] Gartner, Gartner Forecasts Worldwide GenAI Spending to Reach $644 Billion in 2025, 2025: https://www.gartner.com/en/newsroom/press-releases/2025-03-31-gartner-forecasts-worldwide-genai-spending-to-reach-644-billion-in-2025
[77] Visa, Biannual Threats Report Spring 2025, 2025: https://corporate.visa.com/content/dam/VCOM/corporate/solutions/documents/visa-perc-biannual-report-spring-2025.pdf
[78] Capgemini, Account-to-account payments and instant payments set to spark new wave of innovation, 2025: https://www.capgemini.com/wp-content/uploads/2024/09/09_10_World-Payments-Report-2025-Press-Release-1.pdf
[79] Juniper Research, A2A Transaction Value to Reach $195 Trillion in 2030 Globally, Driven by Advanced Value-added Services, 2025: https://www.juniperresearch.com/research/fintech-payments/emerging-payments/a2a-payments-research-report/
[80] FT Advisor, Investment scam losses hit £144mn in 2024, 2025: https://www.ftadviser.com/fraud/2025/6/2/investment-scam-losses-hit-144mn-in-2024/

### 3. Cross-border volumes grow – as does their complexity

Across the industry, there is clear consensus that cross-border flows will continue to grow at high single-digit rates. Global cross-border payments reached ~US$195 trillion in 2024,[81] and are forecast to hit US$290 trillion by 2030.[82] Meanwhile, the Financial Stability Board's 2024 KPI report shows limited progress so far against the G20 targets on cost, speed and transparency,[83] underscoring sustained frictions that criminals exploit across jurisdictions.

In the Baltics, cross-border corridors now represent the majority of card fraud value. Intra-EU flows exploit weaker authentication, while crypto-linked transfers remain a recurring risk vector. Banks stress the need for richer shared intelligence – across both borders and rails – to track mule networks in real time.

### 4. Regulation tightens – increased liabilities, more real-time controls

At the same time, regulation is tightening. PSD3 and the new EU Payment Services Regulation (PSR) – expected to become effective from 2026 – will shift fraud liability toward financial institutions and, for impersonation scams, extend partial responsibility to telecom and digital-platform intermediaries. The IPR requires instant-payment infrastructure by 2025, and Markets in Crypto-Assets Regulation (MiCA) and Financial Data Access Regulation (FIDA) extend compliance to crypto and open finance. Risk management leaders in the Baltics describe the effort to stay ahead as a 'regulatory triathlon' – with multiple directives demanding daily data sharing, proactive reimbursement, and continuous fraud scanning.

### 5. Consumer expectations are up – switching costs are down

Digital banks and fintechs with frictionless multi-factor authentication are raising the bar on customer experience, while incumbents that fail to harmonise experience and security risk sizable market-share erosion as switching costs fall. Consumers now expect payments that are instant, effortless, and infallibly secure. Plaid's 2025 Fintech Effect report confirms that trust and brand loyalty are no longer sufficient: consumers demand instant onboarding, personalised guidance, AI-powered insights, and friction-free payments, and they will switch providers over the quality of their digital experience.[84]

In Nordic-Baltic markets where digital loyalty is thin, that means one poor fraud incident – or one inappropriately blocked payment – can trigger churn. Several CROs framed this paradox clearly: "Too little control and we lose funds; too much and we lose customers." Meeting these expectations while maintaining robust security will be a key differentiator in the years ahead. Interviewees universally acknowledge the tension: one described the equilibrium as "always having a dissatisfied cohort – either those blocked too much or those who suffered losses asking 'why didn't you block?'". Another emphasised that "no transactions means no fraud, but that never works for merchants".

The solution, according to multiple CROs, lies in continuous precision and detection rate improvements, contextual authorisation policies (e.g., more lenient in travel contexts, firmer for online subscriptions), and tight coupling of customer experience and fraud functions. Yet few Baltic institutions have systematically modelled the friction-versus-fraud trade off. Many adjust controls reactively when losses or complaints surge, rather than proactively calibrating them based on cohort-level risk scoring and customer lifetime value.

[81] Payspace, Global Cross-Border Payment Statistics 2024, 2025: https://payspacemagazine.com/statistics/global-cross-border-payment-statistics-2024/
[82] EY, Beyond borders: capturing growth in the dynamic cross-border payments market, 2024: https://www.ey.com/content/dam/ey-unified-site/ey-com/en-gl/industries/wealth-asset-management/documents/ey-gl-banking-beyond-borders-10-2024.pdf
[83] Financial Stability Board, Annual Progress Report on Meeting the Targets for Cross-border Payments: 2024 Report on Key Performance Indicators, 2024: https://www.fsb.org/2024/10/annual-progress-report-on-meeting-the-targets-for-cross-border-payments-2024-report-on-key-performance-indicators/
[84] Plaid, The Fintech Effect, 2025: https://downloads.ctfassets.net/ss5kfr270og3/51PwXCi34K9wWdAoF8IFyX/4bec984c68551f07c175cf998dab1667/US_Fintech_Effect_2025.pdf?form=2008

## 6. New rails and assets – introducing new risks and vulnerabilities

New and alternative payment methods – such as virtual currencies, central bank digital currencies (CBDCs), buy-now-pay-later (BNPL), stablecoins, and super-app digital wallets – are emerging at an accelerating pace. Digital wallets are projected to become the primary online payment method in Europe by 2030, accounting for 40% of transactions,[85] and by 2026, over 5.2 billion people globally (more than 60% of the world's population) are expected to be using digital wallets.[86] Also, alternative payment methods such as BNPL have achieved rapid penetration, with nearly 50% of Europeans aged 18-34 having used a BNPL solution, drawn by the flexibility of deferred payment.[87]

Meanwhile, cryptocurrencies and stablecoins are entering institutional finance, with blockchain technologies enabling faster, cheaper, and automated international transactions through smart contracts. Over 90% of the world's central banks are studying the possibility of issuing CBDCs, and 60% are already performing tests or proofs of concept.[88] Also, frameworks such as the Digital Euro are expected to require PSPs to integrate CBDCs into payment flows in the coming years, carrying significant implications for fraud prevention, AML compliance, and monetary policy transmission. MiCA now regulates stablecoin issuers, requiring real reserves equivalent to amounts in circulation and formal registration, aiming to reassure users while encouraging innovation within a secure framework.

Baltic institutions agree that agility will define resilience. Yet many cite long vendor-approval cycles and legacy core systems as inhibiting innovation.

As one acquirer put it: "Regulators must approve faster so we can evolve as fast as the fraudsters." Another interviewee emphasised that "cost saving and fraud management are not best friends," and that upfront investment in advanced tooling (e.g., Featurespace over cheaper alternatives) saves more overall by enabling better quality business and compliance. The challenge is acute for smaller, younger acquirers, where a few bad actors can materially skew fraud ratios, forcing aggressive offboarding and caps to stay within scheme thresholds. For the industry as a whole, the imperative is clear: institutions must adopt a portfolio view that integrates new payment methods into unified fraud frameworks, leveraging multi-rail transaction data, advanced AI scoring, and cross-sector collaboration to detect and mitigate emerging threats before they scale.


[85] Consultancy EU, Payments Pulse: payments and fintech priorities to watch in 2025, 2025: https://www.consultancy.eu/news/11879/payments-pulse-payments-and-fintech-priorities-to-watch-in-2025
[86] Finextra, The future of payments in major global markets: A mid-decade review, 2025: https://www.finextra.com/researcharticle/348/the-future-of-payments-in-major-global-markets-a-mid-decade-review
[87] TrusTech, The 5 Digital Payment Trends for 2025, 2025: https://www.trustech-event.com/en/event/news/digital-payment-trends-2025
[88] PCMI, Why Central Bank Digital Currencies May Be the Next Disruptor in Payments, 2025: https://paymentscmi.com/insights/market-research-data-central-bank-digital-currencies-cbdcs/

## How well prepared are the Baltics?

Given the complexity and dynamism of the risk environment across the Baltics, there are several dimensions to being well prepared, including:

### 1. People and organisation

Interviews suggest that most Baltic institutions recognise their fraud defences remain fragmented. Respondents frequently described siloed, 'disjointed' operations – such as separate fraud units for issuing, acquiring, and A2A transactions, all running independently, often with limited data sharing or joint oversight. One bank admitted its fraud, disputes, and reimbursement processes "run on parallel tracks", while another noted that card monitoring is handled offshore and disconnected from local A2A fraud management. Several institutions have recently reorganised their financial-crime functions to unite AML and fraud, but most concede that full integration across channels, products, and governance lines is still to come.

Resource constraints add pressure. Smaller acquirers called their fraud workload "a heavy lift," with up to half their staff engaged in compliance and chargeback management. Institutions agreed that overall talent is not the issue – capacity does exist. But without a joined-up structure and clear data ownership, even skilled staff struggle to respond quickly to new threats. A common theme was that success now requires cross-functional teams rather than standalone 'fraud departments'.

### 2. Data and technology

Legacy infrastructure emerged as one of the big barriers. Most institutions report fragmented technology stacks and limited real-time data integration (e.g., different systems for A2A vs. cards), with multiple detection systems and manual case pipelines that prevent real-time insight. Several respondents rated their current capability "below mid-level," acknowledging that controls work at the transaction layer but not at the customer level.

Others said their fraud and cyber tools do not yet connect to CRM channels, limiting the ability to warn clients in-app or via alerts.

Institutions investing in upgrades are on multi-year journeys. Most aim to create unified data layers for ML-enabled scoring and customer-risk models, yet development timelines extend 12-18 months. Also, AI adoption remains uneven: some banks use it only for alert filtering; others have begun integrating behavioural analytics or external vendor models. One participant described AI as "valuable but over-hyped – precision is still low without strong data". Another pointed to alert fatigue, noting that "the issue isn't false negatives anymore, it's too many false positives slowing review". Meanwhile, smaller payment firms face the opposite problem – too few transactions to train effective models.

Regulatory expectations for near real-time reporting remain difficult to meet. While guidelines now require continuous data feeds to national CERTs, several institutions admit legacy IT cannot yet deliver the granularity or speed regulators expect. Respondents across markets voiced concern that, without faster modernisation, compliance deadlines under PSD3 and the Instant Payments Regulation will outpace system capability.

One interviewee summarised bluntly: "Our data runs faster than our governance".

### 3. Governance and regulatory alignment

Process fragmentation mirrors technology gaps. Fraud detection, customer remediation, and reimbursement workflows are often manual or inconsistently applied across channels. One interviewee said, "We still manage cases over email; our process works but isn't scalable". Another mentioned that reimbursement policies are incomplete while liability thresholds under upcoming rules remain unclear.

Regulators' expectations for proactive prevention – real-time blocking, standardised case metrics, and cross-bank sharing – are outpacing current practice. Several financial-crime leaders admitted limited readiness for the PSD3 liability shift, describing their institutions as only "partially prepared". Others have started building reimbursement processes but hesitate to compensate too broadly, warning this could incentivise opportunistic claims. Sector-wide, governance remains compliance-driven rather than risk-intelligence-led. New rules are interpreted narrowly to satisfy audits rather than to drive innovation – a gap the region must close.

Regulators are pushing for clearer legal frameworks that enable banks to block suspicious transactions proactively, even when strong customer authentication is present. Current legislation provides blocking authority primarily for anti-money laundering concerns, but regulators argue that fraud-specific blocking powers are essential, emphasising that, while smooth payment experiences remain important, the industry must accept that effective fraud prevention will require some "collateral damage" in the form of false positives – a paradigm shift from the frictionless payment philosophy that has dominated digital banking strategy.

### 4. Partnerships and collective initiatives

Even amid these constraints, collaboration is gaining pace. Multiple respondents highlighted active industry working groups linking major banks, central banks, and law enforcement, designed to share fraud typologies and coordinate responses to APP scams.

One participant spoke of a forthcoming cross-institution data-exchange platform modelled on existing regional prototypes – a clear step toward systemic intelligence sharing.

Telecom partnerships are expanding as well. Several banks credited joint efforts to block spoofed international calls for significantly reducing vishing attempts. Others referenced pan-Nordic programmes on offline card acceptance and crisis resilience. Regulatory bodies across the region are also issuing clearer standards – some require real-time fraud reporting to national CERTs or dedicated fraud-prevention officers inside each institution. Despite uneven implementation, these initiatives show commitment to collective resilience and transparency.

## A mixed outlook – and a clear need for collaboration

Interviewees uniformly view transformation as achievable but challenging. Many conceded the Baltic sector is "behind on integration" yet simultaneously praised its agility, small-market cooperation, and regulatory engagement. Most predict meaningful progress within two to three years, provided institutions continue investing in unified data, joint monitoring, and smarter use of AI.

Across interviews, a revealing consensus emerged: less optimistic about the industry, confident about the institution. This dichotomy should motivate regional coordination rather than complacency. Each institution may be improving, yet systemic resilience depends on the slowest mover. Encouragingly, most leaders conclude equilibrium is achievable within three years if people, data, and processes evolve in tandem and collaboration expands.

## Four imperatives for sustainable success

Based on our research and relationships across the Baltics, and drawing on VCA's experience from across the global ecosystem, we believe there are four imperatives for the region to achieve and retain a state of equilibrium:

**IMPERATIVE #1**
**Shift from institution-only to ecosystem defences**

### WHAT

- Formalise cross-sector forums that include banks, telcos, payment platforms, CERTs, and law enforcement
- Launch or join real-time intelligence sharing platforms
- Standardize evidence and reporting for APP fraud across institutions

### WHY

Breaking down silos and sharing actionable intelligence is essential to outpace organised fraud rings and respond to regulatory demands for real-time data.

**IMPERATIVE #2**
**Build for explainable real-time controls and behavioural monitoring**

### WHAT

- Deploy layered, AI-driven fraud detection, integrating customer profiling, device intelligence, and behavioural biometrics – and prioritise 'digital fingerprint' capabilities that detect when legitimate credentials are being used by someone other than the account holder
- Ensure instant interventions (alerts, blocks, customer outreach) are routed to CRM/app channels
- Automate case evidence for regulatory audits and reimbursement claims

### WHY

PSD3, PSR, and IPR require real-time, explainable controls – manual reviews alone will not scale.

**IMPERATIVE #3**
**Eliminate the 'manual-review cliff'**

### WHAT

- Invest in orchestration platforms that process alerts, adapt thresholds, and assemble audit-ready case files automatically
- Benchmark current manual review volumes and set targets for automation (e.g., reduce manual reviews by 50% within 12 months)
- Prepare for PSD3/PSR reimbursement regimes by dry-running sender/receiver bank workflows

### WHY

Without automation, regulatory changes will force unsustainable staffing increases and operational bottlenecks.

**IMPERATIVE #4**
**Treat resilience as a product feature**

### WHAT

- Complete offline card acceptance upgrades and crisis runbooks for payment continuity
- Establish 24/7 hotlines between fraud teams and telecom/network operators
- Test and communicate resilience measures to customers (e.g., what happens during outages or cyber incidents)

### WHY

Customers and regulators will judge providers on their ability to maintain secure payments under stress – not just in normal conditions.

# How Visa can help

The Baltic region has emerged as a digital payments leader, pioneering instant A2A transfers and building one of Europe's most dynamic fintech ecosystems. Yet that same digital maturity has reshaped the fraud landscape. The threat has evolved from traditional card-not-present fraud toward authorised push payment scams and social-engineering attacks that weaponise speed, trust, and the irreversibility of real-time rails. Investment fraud and telephone scams now dominate losses across Estonia, Latvia, and Lithuania, with criminals deploying AI-generated voice cloning, deepfake impersonation, and organised money-mule networks. At the same time, regulatory expectations have shifted decisively – from best efforts to accountability by design.

Navigating this environment requires institutions to balance three competing imperatives: maintaining the speed and convenience that customers expect, deploying robust security controls without generating excessive false positives, and demonstrating measurable return on investment from prevention measures.

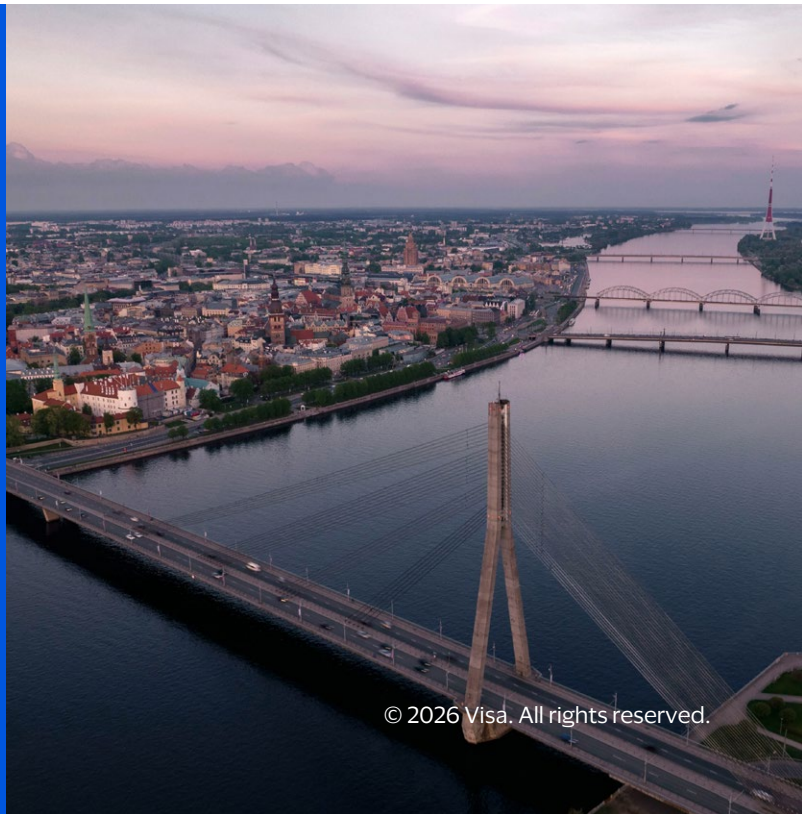
Through Visa Consulting & Analytics (VCA) and Visa Implementation Services (VIS), Visa delivers an end-to-end approach, combining advanced risk technology, consulting expertise, and implementation capabilities. With our support, institutions can reduce fraud, prevent false declines, and achieve regulatory compliance across both card and A2A rails.

Our integrated delivery covers:

- Fraud equilibrium scorecards balancing speed, security, and savings, delivered through three phases:
  - Phase 1 – use broad benchmarks for high-level maturity assessment
  - Phase 2 – develop a comprehensive scorecard that includes detailed diagnostics, full metric sets, and tailored recommendations
  - Phase 3 – apply the scorecard for ongoing monitoring, tracking improvements over time, and benchmarking against peers
- Operational optimization
- Regulatory readiness and model tuning, including PSD3/PSR reimbursement playbooks
- Fraud stack integration blueprints (customer-level risk, CRM/app orchestration)
- Cybersecurity advisory
- Cross-platform integration and orchestration

Underpinning this is Visa's risk product suite, providing AI-driven fraud detection, authentication, and orchestration capabilities that integrate seamlessly with client ecosystems. Together, VCA, VIS, and Visa's technology deliver measurable outcomes that minimise fraud losses, reduce false positives, and eliminate operational drag.

Visa delivers an end-to-end fraud prevention approach that unites advanced risk technology, consulting expertise, and hands-on implementation.



All brand names, logos and/or trademarks are the property of their respective owners, are used for identification purposes only, and do not necessarily imply product endorsement or affiliation with Visa.

These materials and best practice recommendations are provided for informational purposes only and should not be relied upon for marketing, legal, regulatory or other advice. Materials and recommendations should be independently evaluated in light of your specific business needs and any applicable laws and regulations. Visa is not responsible for your use of the marketing materials, best practice recommendations, or other information, including errors of any kind, contained in this document.

Case studies, comparisons, statistics, research and recommendations are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. Visa neither makes any warranty or representation as to the completeness or accuracy of the information within this document, nor assumes any liability or responsibility that may result from reliance on such information. The Information contained herein is not intended as investment or legal advice, and readers are encouraged to seek the advice of a competent professional where such advice is required.