

IOTA Forum on Combating VAT Fraud

“VAT fraud cases in import and export”

FEEDBACK SESSION

Group Discussion Session 1

New/significant VAT Fraud Trends



IOTA Forum on Combating VAT Fraud

Question 1

What new or emerging VAT fraud schemes are being observed across goods, services, and intangibles? In particular, we would greatly appreciate your insights in VAT fraud in cross-border trade and e-commerce (e.g. involving Alternative Payment Systems such as cryptocurrencies, or Electronic Money Institutions).

IOTA FORUM 6 – 7 May 2026

GROUP 1

FEEDBACK ON QUESTION 1

Digital and online activities (e-commerce, digital content, influencers) present growing VAT compliance risks, particularly among unregistered or hard-to-identify suppliers.

Cryptocurrency usage is increasingly observed in tourism, digital services, and property transactions, complicating traceability and valuation despite growing access to related data.

Identification of the true supplier remains challenging due to cross-border structures, intermediaries, and service providers located outside the jurisdiction.

False or paper-only invoicing schemes persist, even where mandatory e-invoicing is in place, highlighting limits of form-based controls.

IOTA Forum on Combating VAT Fraud

Question 1

What new or emerging VAT fraud schemes are being observed across goods, services, and intangibles? In particular, we would greatly appreciate your insights in VAT fraud in cross-border trade and e-commerce (e.g. involving Alternative Payment Systems such as cryptocurrencies, or Electronic Money Institutions).

IOTA FORUM 6 – 7 May 2026

GROUP 1

FEEDBACK ON QUESTION 1

- **Mandatory e-invoicing and real-time data exchange**

significantly improve visibility and early detection, but data quality and misuse remain key risks.

- **Limited transparency of payments and supply chains** continues to hinder effective matching between transactions, VAT returns, and customs data.

- **Increased use of third-party data** (CESOP, DACs, card data, customs information) strengthens risk analysis, especially when integrated across tax and customs administrations.

- **Unregistered economic activity** (e.g. short-term rentals, vehicle trading, influencers) remains a recurring vulnerability.

Key message: Digitalisation improves detection, but fraud adapts quickly; effective control depends on data integration, substance-based analysis, and coordinated tax–customs approaches.

IOTA Forum on Combating VAT Fraud

Question 2

How have fraudsters adapted their methods in response to the increased use of e-invoicing, real time reporting and data analytics by tax administrations? And have you observed such adaptations in your own work?

IOTA FORUM 6 – 7 May 2026

GROUP 2

FEEDBACK ON QUESTION 2

- **Displacement of payment channels:** Shift from traditional banks to virtual banks, e-money, and layered payment structures to reduce monitoring; cashless systems increase traceability but do not eliminate fraud.
 - **Identity abuse:** Use of stolen, borrowed, or synthetic identities
 - **Transaction fragmentation (smurfing):** Splitting transactions below reporting or control thresholds to evade detection.
 - **Misclassification of transactions:** Simulating B2B transactions that are effectively B2C to circumvent VAT obligations, particularly in digital trade.
 - **Exploitation of existing legal entities:** Acquisition of older bona fide companies to gain credible VAT numbers, compliance history, and retroactive access.
 - **Adaptation to e-invoicing:** Fraud persists through fake invoices, but real-time data significantly improves visibility, detection, and feedback to tax administrations.
 - **Cross-border layering:** Moving activities abroad or adding jurisdictions to exploit regulatory gaps and delay enforcement.
 - **Multi-tax fraud:** Single schemes targeting VAT, income taxes, and other levies simultaneously, increasing complexity and impact.
- Key message:** Modern fraud is network-based, cross-border, and multi-tax, requiring real-time data, integrated controls, and advanced analytics rather than isolated, rule-based checks.

IOTA Forum on Combating VAT Fraud

Question 3

Which sectors or transaction types (for example green energy, small parcels, marketplaces) currently present the highest emerging risk, and what early warning indicators do you monitor?

IOTA FORUM 6 – 7 May 2026

GROUP ONLINE

FEEDBACK ON QUESTION 3

HIGHEST-RISK SECTORS AND EARLY WARNING INDICATORS

High-Risk Sectors

Data centres, crypto mining, digital services, and e-commerce marketplaces are identified as sectors with high emerging VAT risks.

Complex Payment Ecosystems

Payment ecosystems involving PSPs and EMLs complicate transaction flows and increase VAT risk exposure.

Early Warning Indicators

Indicators include high input VAT deductions, frequent business model changes, reliance on non-EU infrastructure, and crypto payment use.

Role of Intelligence

Digital forensics, criminal investigations, and cross-border cooperation are crucial for risk detection and prioritization.