Risk profile guide

Money Laundering and Terrorist Financing

Use of the Second-Hand Mobile Device Trade by Organised Crime

October 2025

SEPBLAC

This risk profile guide on the prevention of money laundering and terrorist financing has been prepared for informational and guidance purposes only.

Its use does not exempt obliged entities from the strict fulfilment of their legal obligations, nor from applying their own risk analysis and assessment criteria in accordance with their activity, structure, and business model. Responsibility for the correct application of anti–money laundering and counter–terrorist financing (AML/CFT) regulations, as well as for any implementation or interpretation of the contents herein, lies exclusively with the obliged entities.

Contents

General context

What is Crime-as-a-Service?

In certain cases, criminal organisations do not carry out the money laundering process directly. Instead, they outsource this activity to specialised professionals.

These experts offer their services as a form of money laundering outsourcing, accessible to any criminal group or organisation that needs it or lacks the necessary infrastructure to conduct it internally.

These professionals market money laundering as a service-for-hire—what might be called money laundering-as-a-service—in exchange for a commission.

In doing so, they completely separate the ownership of the criminal proceeds from the ownership of the financial instruments through which such funds circulate.

Which sectors do these "professionals" target?

Fundamentally, these are sectors where there is a lack of transparency or where it is difficult to determine the true value of the goods or services being traded. These include sectors dealing in second-hand items—such as used clothing, car sales, and electronic products—sectors handling high-value goods, such as jewellery and precious metals, and finally, activities like consultancy or advertising, where the value of the service provided is difficult for an external observer to audit

Why the mobile phone sector?

This market has experienced sustained growth in recent years, driven by a shift in consumer preferences towards second-hand devices. This trend is explained by factors such as more affordable prices, improved product quality, broader after-sales services, easier access to device financing, and increased awareness of sustainability. These conditions make it relatively easy to justify the movement of substantial sums of money through the financial system, supported by documentation or invoices that are difficult to verify, given that the goods being traded are second-hand

Risk indicators

GROUP 1

- **Private limited companies operating small retail businesses**

- **Self-employed individuals working as sole traders**

- Newly established businesses engaged in the purchase, sale and/or repair of mobile devices
- Use of bank accounts with high transactional intensity—both incoming and outgoing—over short periods, aimed at obscuring links to the underlying criminal organisation
- Large cash deposits of unexplained origin, potentially connected to illicit activities
- Absence of typical debits associated with legitimate economic activity, such as utilities, social security contributions, salaries, fees or taxes
- Outgoing transfers to domestic accounts held by companies classified under GROUP 2

GROUP 2-3

- **Intermediary Companies or Facilitators**

- Companies presenting a stronger appearance of business activity and greater stability over time compared to those in GROUP 1
- Incoming domestic transfers from entities classified under GROUP 1
- Domestic fund movements between their own accounts across various financial institutions, as well as with accounts held by other similar shell companies
- Business infrastructure (facilities and staff) insufficient to support the high volume of commercial activity they appear to conduct
- No genuine online presence, or if one exists, it is non-functional in practice

GROUP 4

- **Companies Registered Abroad**

- Incoming transfers of funds from entities classified under GROUP 2
- Identifiable links to criminal organisations located in their country of registration

SEPBLAC

Coordinated Financial Prevention

Frontline detection

Obliged entities occupy a strategic position in identifying suspicious operations. Once such activity is detected, it is crucial that reports submitted to Sepblac include a concise summary that, where applicable, answers the questions: who, what, when, where, how, and how much (amount). This summary—together with the risk mapping information provided by entities reporting via CTL, and the accurate identification of all parties involved—facilitates the prioritisation and connection of suspicious operations reported by different obliged entities, as well as the identification of emerging trends.

Behind the Scenes

Sepblac receives information from multiple sources, which it structures and labels to carry out both operational and strategic analyses. Following the receipt of suspicious transaction reports identifying (1) small retail shops trading in second-hand mobile devices that were depositing large volumes of cash, and (2) intermediary companies dealing in second-hand mobile devices that were conducting domestic and international fund transfers, which may correspond to a potential VAT carousel fraud, Sepblac initiated a strategic analysis of the sector.

The use of network analysis tools enables the identification of natural persons and/or legal entities with a high degree of interconnection, facilitating the prioritisation of subjects for operational analysis. Within the framework of these analyses, recurring risk indicators are identified and subsequently integrated into the strategic analysis model.

SEPBLAC