



European
Commission

E-Money

SNRA

SNRA – E-money

Definition

- **Second E-Money Directive (EMD2, 2009/110/EC)**
- **key characteristic: pre-paid nature**

Clasification

- **Reloadable / non-reloadable**
- **linked to other e-money schemes (i.e. cards linked to online accounts) / cards with basic bank account features**
- **pre-paid by the user (payer)/ by a third-party**

Relevant actors

- **the issuer: entity which 'sells' e-money to the customer**
- **the distributor: entity other than the issuer that can distribute or redeem e-money on behalf of the issuer**
- **the agent: entity that acts on behalf of the EMI through which an EMI can carry out payment services activities in another Member State**

SNRA – Threats TF

TF


- **attractive for terrorist groups**
- **Terrorist activities easily financed - low level of planning/expertise**
- **Still less attractive than cash**
- **TF risk: Significant/Very significant**

SNRA – Threats ML

ML

- **FIUs - purchase of multiple prepaid cards of large amounts**
- **LEAs - cases where the proceeds of drug trafficking were laundered by prepaid cards**
- **Same as TF - Still less attractive than cash**
- **ML risk: Significant/Very significant**

SNRA – Vulnerabilities (Risk Exposure)

- **Anonymous Transactions - purchase of multiple prepaid cards of large amounts**
- **Risk factors:**
 - structure of the product,
 - operator
 - capability to identify and report suspicious transactions
- **Supervisors**  **capability is uneven from one operator to another**

SNRA – Vulnerabilities (Risk awareness)

- **Financial inclusion** → **Risk awareness in the sector (TF&ML abuses as marginal)**
- **CDD exemption** → **Monitoring of transactions not sufficient**
- **Risk awareness tend to increase.**
- **In general - Not harmonized sector**
 - Big players with robust assessments
 - Small player with limited resources

SNRA – Vulnerabilities

legal framework and controls

- **SNRA 2017 AML/CFT framework, e-money products benefit from an exemption regime which allows CDD not to be applied when specific conditions are fulfilled**
- **doubt regarding the effectiveness of AML/CFT framework in the absence of identification measures**

SNRA – Vulnerabilities

Conclusions:

Anonymity  *e-money is inherently exposed to TF&ML vulnerability*

Increasing level of awareness but not sufficient (FIUs have to acquire more data from suspicious transactions)

vulnerability: significant/very significant.

Mitigating measures

*Proposal for amending Directive (EU) 2015/849 (COM(2016)450). **Limiting the anonymity of prepaid instruments:***

- **lower thresholds in respect of non-reloadable prepaid payment instruments.**
- **suppress the CDD exemption for online use of prepaid cards.**
- *ESAs analysis of operational AML/CFT risks linked to the business/business model in the e-money sector.*