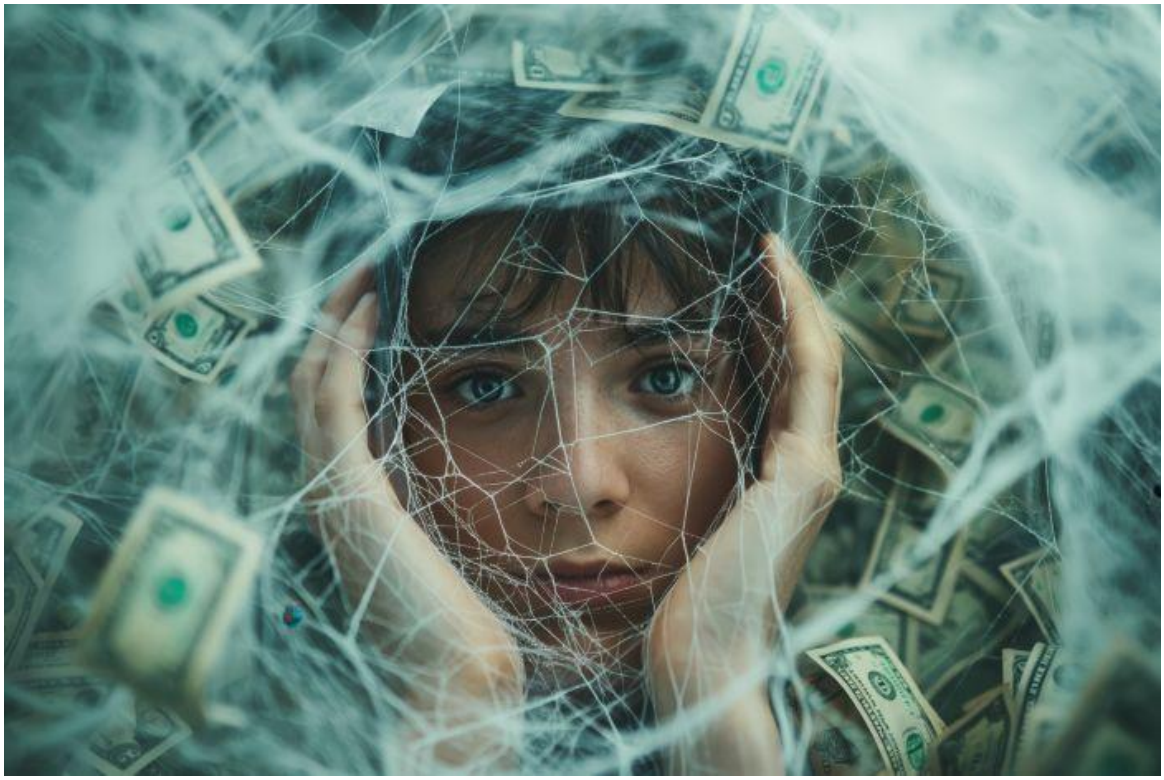
KS6 (The Knowledge Series)

The Hidden Threat : Perspectives on evolving Money Laundering and Trade Fraud Challenges

By Ganesh Vishwanathan
August 25, 2025

"Criminal networks fuel their operations through corruption and money laundering, creating a hidden financial system that weakens economies and erodes trust in governance structures.

2025 European Union Serious and Organized Crime Threat Assessment



Overview

Criminal organisations rely on an interconnected and international financial system to support their illegal schemes. Financial crime is escalating globally, with sophisticated methods and increasing losses, necessitating enhanced collaboration among financial institutions and authorities. Trade fraud challenges stem from fraudsters exploiting complex, document-heavy processes, a lack of transparency, and fragmented data across jurisdictions, leading to risks like forged documents, misrepresented data, and unauthorized transactions

Perhaps the greatest indicator of advancements in financial crime today is the emergence of the ***crime as a service model***, with criminal groups pivoting from vertical

to horizontal monopolies specializing in what illicit acts they perform best. Criminal networks have created intricate systems to expand operations and accumulate wealth from illegal activities, often employing a diverse array of methods and utilizing new technologies. Online environments like e-commerce further empower criminal networks to capitalize on opportunities across borders in geographies that were once beyond their control or access, conducting operations around the world with precision, speed, and agility. Advanced criminal networks are especially prevalent within money laundering operation.

What is worrying is that money laundered through legitimate financial system including, inter-alia through TBML, SBML and TBTF are now increasingly using trade mule accounts, a new concept and direction.

Emerging technologies like AI and LLMs improve the sophistication of financial crime not by the year or the month but by the day or the hour, while encrypted social media channels and the dark web act as criminal classrooms, training grounds, Genius Bars, and app stores for bad actors to hone their skills, craft their attacks, and identify vulnerabilities and victims. Increasingly, the world of TBML is being controlled by Organized Criminal Groups , rather than bad apples amongst Importers and Exporters.

Let us now look at the results of a survey carried out recently.

> Fraudsters and money launderers are focussed on the fragility of the human control methods and the current reliance on manual processes and paper documents.

Weight of Shadows

- $3.1 trillion in illicit funds moved through the financial system in 2023.
- Projected losses from scams and fraud reached $485.6 billion.
- 78% of professionals believe criminal enterprises are more sophisticated at laundering money than financial institutions (FIs) at detecting it.
- 71% agree that fraud is linked to illegal activities like human trafficking, wildlife trafficking and terrorism financing.

Unseen Battle Against Financial Crime

- 77% of FIs believe they are winning the war against financial crime.
- 71% report an increase in fraud attempts at their institutions.
- 59% say losses due to fraud are increasing year-over-year.

- Only 41% describe their organization as "very effective" at combatting financial crime.

Rethinking Detection Strategies

- 68% of FIs spend $10 million or more annually on financial crime detection technologies.
- 76% use behavior-based analysis for financial crime detection.
- Nearly half (47%) report losing $10 million or more to fraud annually.
- FIs that invest in behavior-based analysis are less likely to lose substantial sums to fraud.

> A best practice approach to Trade Finance fraud and money laundering needs to focus on multiple stages in the monitoring and control lifecycle, with the ability to add more internal and external contextual information.

Financial Crime 2.0

- 84% of professionals agree that combatting the Dark Economy is important.
- 78% say criminal enterprises are more sophisticated at laundering money than FIs at detecting it.
- Emerging technologies like AI, social media, and dark web forums have increased the sophistication of financial crimes.

It Takes a Network to Stop a Network

- 61% of FIs say law enforcement often gets involved in suspected money laundering cases.
- 88% believe law enforcement should do more when Suspicious Activity Reports (SARs) are filed.
- 58% share information on suspicious accounts with other FIs weekly or more frequently.

Path Forward

FIs face increasing fraud and Money Laundering attempts and losses each year. The shift away from currency based laundering towards asset-based methods like TBML represent a deeper challenge for law enforcement and financial institutions.

Collaboration among FIs, regulatory authorities, and law enforcement is essential to combat financial crime effectively but needs improvement.

Emerging fraud and Money Laundering technologies pose significant challenges, necessitating a proactive approach to information sharing and strategy adaptation.

Source :

1. Private Company Research Poll : . Respondents were from Fis, manager level and above in US, Canada, France, Germany, Spain, UK, UAE, Sweden, Australia, India, Brazil, Mexico.
2. WTO, IMF, SaaS, GFI, World Bank, FinCEN, FIU(India)
3. FinCrime Fighters Forum Discussions
4. Author personal experiences
5. Information in Public Domain