USD 439 million recovered in Interpol-led operation| New trade-based money laundering modus operandi| Beneficial ownership obligations and more

October, 2025

TOP STORY

Operation HAECHI VI: USD 439 million recovered in global financial crime operation

By Neha Treesa Joy

An Interpol-led operation across 40 countries and territories has resulted in the recovery of USD 342 million in government-backed currencies, along with USD 97 million in physical and virtual assets.

Operation HAECHI is an Interpol-coordinated global operation series focused on tracking and seizing money lost to fraudulent schemes. It began in 2020, led by the Interpol Financial Crime and Anti-Corruption Centre (IFCACC) and the Korean National Police Agency (KNPA). The series has since expanded globally from Asia-Pacific in its early phases to full worldwide participation by HAECHI VI.

Operation HAECHI VI, which took place between April and August 2025, targeted seven types of cyber-enabled financial fraud: voice phishing, romance scams, online sextortion, investment fraud, business email compromise, money laundering associated with illegal online gambling, and e-commerce fraud. According to Interpol, the investigation team of this operation was able to block more than 68,000 associated bank accounts and freeze almost 400 cryptocurrency wallets. Additionally, around USD 16 million in suspected illicit profits was recovered from cryptocurrency wallets.

HAECHI VI was a collaborative initiative involving multiple countries, such as Portugal, Thailand, South Korea, Myanmar, etc. In Portugal, authorities dismantled a sophisticated cybercrime network that had breached the national social security system, illegally accessing accounts and altering beneficiaries' bank details to divert welfare payments intended for vulnerable families. In South Korea, rapid coordination through INTERPOL's Global Rapid Intervention of Payments (I-GRIP) mechanism enabled the recovery of USD 3.91 million after a steel company noticed forged shipping documents and funds were traced to a Dubai account.

INTERPOL's Director pro tempore of the Financial Crime and Anti-Corruption Centre, Theos Badege emphasised on collaboration saying

"While many people believe that funds lost to fraud and scams are often irretrievable, the outcomes of HAECHI operations demonstrate that recovery is indeed possible. As one of INTERPOL's flagship financial crime operations, HAECHI is a prime example of how global cooperation can protect communities and safeguard financial systems."

Criminal networks behind fraud schemes often operate across multiple jurisdictions, making it extremely difficult for any single nation to trace, freeze, and recover illicit funds. Collaboration and information sharing among countries can facilitate investigation and dismantle such transnational criminal activities. Global cooperation is essential so that meaningful differences can be made in the fight against cyber-enabled crime.

Source: INTERPOL

NEWS SNIPS FROM AROUND THE WORLD

[Collated from other publishers and sources from the Internet, as referenced after each snippet]

Canada's AML watchdog fines crypto exchange KuCoin for AML deficiencies

The Financial Transactions and Report Analysis Centre of Canada, the country's anti-money laundering agency, has fined Peken Global Limited, the operator of crypto exchange KuCoin, its largest-ever penalty of C$19.6 million ($14.09 million). The Seychelles-based firm failed to register as a foreign money services business, was unable to report large-value transactions of C$10,000 or more, and did not submit suspicious transaction reports as required by financial institutions. The move comes as Canada

prepares for an audit by the Financial Action Task Force in November on its financial crime controls.

Source: Reuters

Authorities dismantle criminal groups laundering money via trade in gold bars

A joint French-Italian investigation team, supported by Eurojust and Europol, dismantled two linked organised crime groups (OCGs) involved in drug trafficking and large-scale money laundering. One network of Syrian and Egyptian origin operated from northern Italy by offering 'crime as a service' through the hawala system, laundering money for other OCGs. This system involves hiding illegal gains through a chain of guarantees or promises to transfer huge sums of money for laundering. The group also purchased and exchanged nearly 100 kilos of gold bars to conceal illegal proceeds. In coordinated operations, 12 suspects were arrested, over 25 locations searched, and assets, including gold, cash, luxury cars, and watches worth around EUR 8 million were seized. The illicit funds involved are estimated to be at least EUR 30 million.

Source: EUROJUST

£5 billion Bitcoin scam busted

A Chinese national pleaded guilty to illegally acquiring and possessing cryptocurrency worth more than £5 billion. She led a large-scale scam in China by cheating 1,28,000 victims and storing stolen funds in bitcoin. She fled China and entered the UK using fake documents and attempted to launder the money by purchasing property. Police stated that the large amount of bitcoin and lack of evidence regarding its acquisition indicated that it was from a criminal source. Bitcoin and other cryptocurrencies are increasingly being used to disguise and transfer assets.

Source: The Times of India

Dutch bank fined for AML failures

Dutch online bank Bunq has been fined 2.6 million Euro by the Netherlands' Central Bank, De Nederlandsche Bank(DCB), for Anti Money Laundering(AML) failures. The investigation revealed that between January 2021 and May 2022, the bank failed to adequately investigate or report suspicious activity across multiple customer files. According to regulators, Bunq did not properly follow up on transaction monitoring alerts, overlooked signs of potential financial crime, and failed to maintain sufficient insight into customers and their transactions, despite earlier warnings about its compliance systems.

Source: Reuters

Chandigarh Police arrest two in lapsed insurance policy fraud

Chandigarh Cyber Crime Police have arrested two individuals from Delhi for defrauding a resident of ₹3 lakh while pretending to renew an expired insurance policy. The accused posed as officials from Bajaj Allianz Insurance Company. Investigations, including technical analysis of mobile numbers and bank accounts, led to their arrests in Noida and Ghaziabad. Authorities recovered multiple mobile phones, SIM cards, ATM cards, and a PAN card from their possession. Both individuals provided information about a suspected mastermind and a network of illegal SIM sellers operating in Noida.

Source: The Indian Express

Investigation Admiral 2.0- tax evasion and money laundering worth 6.5 million euros

The European Public Prosecutor's Office (EPPO) in Riga has brought charges against the suspected large-scale organized criminal scheme that allegedly defrauded the EU and several state budgets of nearly 297 million euro through tax evasion and money laundering. The operation revolved around fraudulent trade in consumer electronics across multiple countries, including Austria, France, Germany and Latvia, where over 400 companies are suspected of being part of the network. The EPPO alleges that the scheme coordinated an elaborate system of fictitious invoicing and cross-border transactions designed to evade VAT payments while laundering the illicit proceeds back into the legal economy.

Source: European Public Prosecutor's Office

EMERGING TRENDS

ED discovers new trade-based money laundering modus operandi

By Shivani S.

On 21st August, 2025, the Directorate of Enforcement (ED) successfully published its first ever Purple Notice through INTERPOL (International Criminal Police Organisation). ED's team discovered a new modus operandi of trade based money laundering during a case investigation, which was shared with INTERPOL's 196 member countries to alert and sensitize global counterparts about emerging trends. A Purple Notice is one of eight types published by Interpol, providing member countries with information on modus operandi, devices and concealment methods used by criminals.

The ED's probe uncovered a well-organised network of domestic and overseas shell companies involved in large-scale money laundering under the disguise of international trade. The criminals exploited trade mechanisms and banking channels by under-invoicing imports, falsely claiming duty-free imports such as semiconductors, forging compliance documents, and conducting circular re-exports through third-country entities to conceal illicit remittances.

This circular trading created a false image of cross-border commerce, thereby facilitating extensive laundering of funds. While the scheme resembled hawala operations, in reality, it operated through formal banking systems, shell companies, and forged trade documents to bypass regulatory detection.

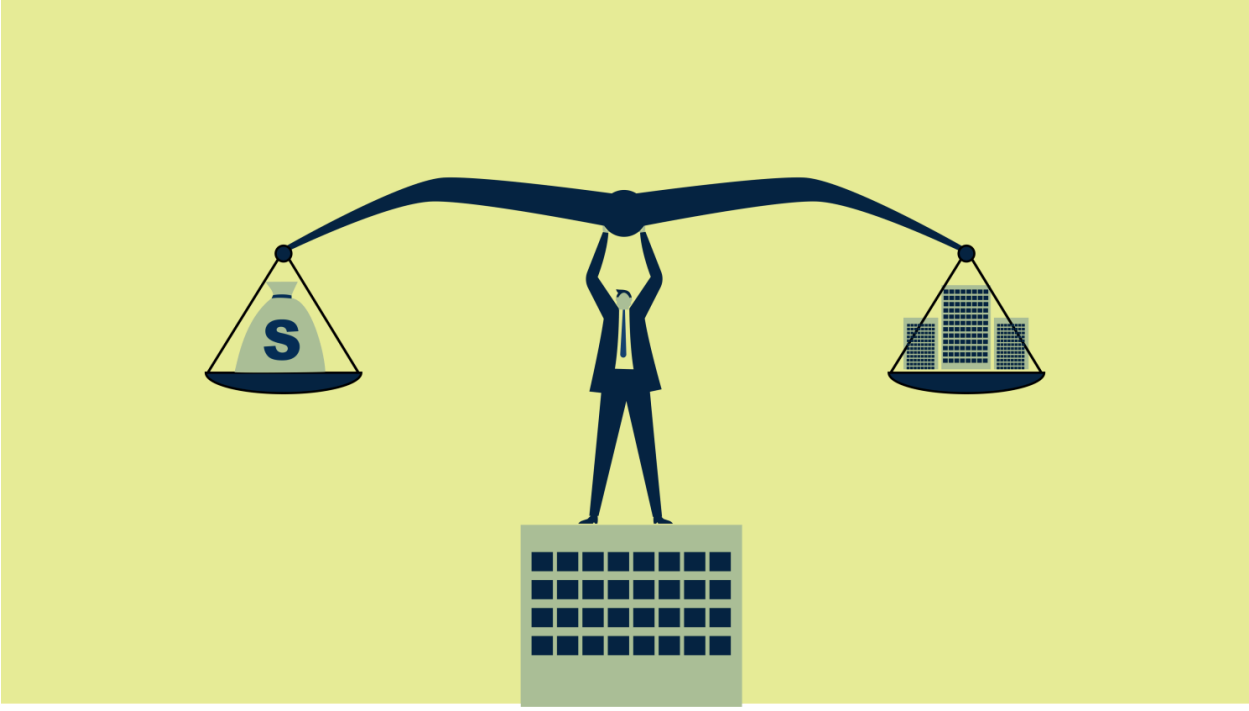
The Purple Notice serves to raise awareness of financial crime risks and sensitise global counterparts of the ED to these emerging money laundering trends. Since money laundering is a complex and transnational crime, international cooperation through informal channels enables tracing assets and gathering relevant information for ongoing investigations. Financial crime methods continue to evolve, and hence, such initiatives are necessary to stay ahead of threats and protect financial institutions. The notice is also a reminder for institutions to improve their compliance framework by investing in technology that can detect and flag suspicious activity.

Source: Enforcement Directorate

DOMAIN MATTERS

How to Strengthen Beneficial Ownership Transparency

By Anna Paulin



As global financial crime becomes more sophisticated, it is crucial to identify Beneficial Owner (BO) information to prevent the misuse of the financial system. Complex ownership structures, cross-border arrangements, and non-transparent nominee relationships continue to facilitate money laundering, terrorist financing, tax fraud, and corruption. Recognising these risks, the Financial Action Task Force (FATF) has revised Recommendation 24 to ensure that BO information is adequate, accurate, and up to date.

Key Pillars for Beneficial Ownership Information

Ensuring the quality of beneficial ownership information requires adherence to three key pillars:

1. Adequate Beneficial Ownership Information: Countries must have mechanisms to ensure that BO information is adequate, including information recorded in company registries. Adequate information should be sufficient to identify the natural person(s) who are the BOs and the means through which they exercise ownership or control. Essential information includes first and last name, nationality, and date of birth.
2. Accurate BO Information: Following the identification of BO, this information must be verified. Under Recommendation 24, verification involves a combination of checks and other processes that a country should adopt at various stages to ensure that the beneficial ownership data is accurate. In case of high risk countries, the verification should be conducted frequently. As a complementary measure, countries may also introduce discrepancy reporting mechanisms to flag inconsistencies between registry data and information collected by legal entities.
3. Up-To-Date BO Information: According to Recommendation 24, countries must set up procedures to ensure that basic ownership data are updated as quickly as possible within a reasonable amount of time. To avoid uncertainty, countries should establish a clear and practical framework that promotes the timely updating of beneficial ownership information. As a best practice, countries may require companies to periodically validate their beneficial ownership information.

Beneficial Ownership Obligations

Once the three fundamental pillars are in place, the role of private sector entities becomes crucial. Financial institutions (FIs) and Virtual Asset Service Providers (VASPs) play a significant role in identifying and verifying beneficial ownership information as part of their Customer Due Diligence (CDD) measures. Under the FATF Recommendations, particularly 10, 22, and 24, FIs and VASPs are required to identify and take reasonable

steps to verify the identity of the BO. During onboarding and throughout the business relationship, they must collect reliable and independent sources of information. VASPs are required to verify the beneficial owners of virtual asset accounts and make sure that transactions don't use anonymity-enhancing techniques that mask ownership.

The revised FATF Recommendation 24 makes clear that countries must adopt comprehensive frameworks that combine disclosure, verification, and timely updates. Collaboration between regulators, financial institutions, and technology providers is vital to ensure accurate identification of beneficial owners. Incorporating these measures into national frameworks helps ensure compliance with international standards and more effective prevention of financial crime.

Source: FATF

Navigate Consulting enables banks and financial institutions to better understand Financial Crime Management and make the most productive use of their AML and Fraud Management systems through training and knowledge sharing.