Insights Papers

January 2026

# Leveraging Partnerships and Technology to Tackle Money Mules

Olivier Kraft and Marta Popyk

RUSI

CENTER FOR FINANCIAL INTEGRITY | ЦЕНТР ФІНАНСОВОЇ ЦІЛІСНОСТІ

## Disclaimer

The content in this publication is provided for general information only. It is not intended to amount to advice on which you should rely. You must obtain professional or specialist advice before taking, or refraining from, any action based on the content in this publication.

The views expressed in this publication are those of the authors, and do not necessarily reflect the views of RUSI or any other institution.

To the fullest extent permitted by law, RUSI shall not be liable for any loss or damage of any nature whether foreseeable or unforeseeable (including, without limitation, in defamation) arising from or in connection with the reproduction, reliance on or use of the publication or any of the information contained in the publication by you or any third party. References to RUSI include its directors, trustees and employees.



RUSI Insights Papers, January 2026

## Publications Team

**Editorial**

Director of Publications: Alice Trouncer

Managing Editor: Sarah Hudson

Assistant Editor: Sophie Boulter

**Design**

Graphic Designer: Lisa Westthorp

**Research Editorial**

Head of Research Governance and Editorial: Elias Forneris

Cover image: Courtesy of Adobe Stock / mitarart

## Get in touch

www.rusi.org

enquiries@rusi.org

+44 (0)207 747 2600

The Royal United Services Institute for Defence and Security

61 Whitehall, London

SW1A 2ET

United Kingdom

## Follow us on

# Overview

On 9 and 10 December 2025, the Centre for Finance and Security at RUSI and the Center for Financial Integrity (CFI) convened a third meeting of the Taskforce on Public–Private Partnership in Fighting Financial Crime in Ukraine. Fifty participants, including representatives from the public and private sectors in Ukraine and a number of international experts, gathered for two days of in-person meetings in Warsaw. The discussions focused on the use of so-called money mules in Ukraine, as well as available mitigation measures offered by public–private partnerships (PPPs) and regulatory technology (RegTech).

Participants developed recommendations for understanding, preventing, detecting and responding to the money mule threat in Ukraine. This Insights Paper summarises the main findings of the meeting. None of the discussions at the meeting are attributable to any specific individual or organisation. Unless otherwise indicated, statements in this paper reflect points raised during the discussions.

# Introduction

As outlined in a recent paper published by the CFI, money mule schemes have become a significant financial crime issue in Ukraine, particularly following the start of Russia's full-scale invasion.

Money mules are individuals whose bank accounts, payment cards or personal data are used to move illicit funds, but who are generally not involved in either the underlying criminal activity generating proceeds or the predicate crimes. Some knowingly allow their accounts to be used in exchange for payment, and some become involved through others' deception or without fully understanding the consequences. In all cases, money mule accounts are used to fragment financial flows and make illicit activity harder to trace.

The CFI paper reviews the impact of the money mule threat on individuals, the financial system and public finances. Estimates suggest that more than UAH 200 billion ($4.8 billion) flows through money mule schemes each year, resulting in up to UAH 50 billion ($1.25 billion) in lost tax revenues. These losses directly affect the resources available for the military, social services and reconstruction.

# Understanding the Threat

A robust understanding of the nature and broader environment of money mule activity was described at the meeting as a prerequisite for an effective response.

## Money Mule Typologies

There is no single money mule profile. While it is often believed that money mules are usually young or elderly, one of the participants reported that individuals aged between 25 and 40 are also increasingly exposed. Several participants distinguished between individuals who are unaware that their accounts are being used for illicit purposes and those who knowingly allow their accounts or payment instruments to be used in exchange for payment. In either case, individuals frequently do not fully understand the legal and financial consequences of such activity.

Recruitment methods discussed included a range of scams and social engineering techniques. For example, certain targets were led to believe that they were assisting displaced persons from Eastern Ukraine who purportedly could not access banking services. Recruitment methods adapt quickly to social conditions and are difficult to counter through static controls.

Participants also highlighted the misuse of social media and messaging platforms in facilitating money mule recruitment. Ukraine's high level of digitalisation was described as amplifying the reach of online advertisements that offer to buy bank cards or accounts, sometimes with falsified bank logos.

In response to these risks, retail banking products for younger customers have been restricted in recent years, particularly accounts available to individuals aged 14–16, who do not face criminal liability under Ukrainian law and might thus be at a higher risk of being targeted to become money mules. However, as indicated above, participants noted that recruitment efforts had shifted towards other age groups.

# Predicate Crimes and Criminal Ecosystems

Participants cautioned against viewing money mules in isolation. Money mule activity was described as one element within broader criminal ecosystems, rather than as an end in itself. Discussions linked money mule schemes to multiple predicate offences generating criminal proceeds, including fraud and tax evasion. The prevalence of informal economic activity and tax evasion contributes to an environment in which money mule schemes can operate, suggesting deeper structural challenges beyond the financial sector.

There was no consensus as to the usual origins and destinations of criminal proceeds laundered through money mule networks in Ukraine, or as to which of the following three categories they most commonly fall under: proceeds generated in Ukraine and retained domestically; proceeds generated outside Ukraine and laundered through Ukrainian accounts; or proceeds generated in Ukraine and transferred abroad.

Transnational organised criminal groups deliberately exploit for money muling jurisdictions where account opening processes are rapid and transaction monitoring is less stringent, as transactions are less traceable in such jurisdictions. Meeting participants agreed that some of Ukraine's financial institutions offer near-instant account opening with limited initial checks, relying primarily on post-onboarding monitoring. They noted that stricter application in Ukraine of know-your-customer (KYC) requirements at the onboarding stage could significantly reduce the misuse of accounts for money muling.

Money mule typologies can provide insight into the structure and sophistication of underlying criminal activity, helping financial institutions and law enforcement to better detect and investigate such activity. For example, empirical research from the Netherlands was cited to illustrate how money mules operate within wider criminal networks. The study, based on bank transaction data, shows that money mules are typically positioned at the periphery of criminal networks and are used to obscure links to organisers. It distinguishes between lower-tech schemes, which rely on a larger number of predominantly domestic money mules, and more sophisticated schemes, which tend to involve fewer mules and greater use of cross-border or business accounts.

## Threat Level

There was no consensus among participants on whether the overall number of money mules in Ukraine was increasing or decreasing. Some participants reported a year-on-year increase in detected cases, while others described changes in typologies and recruitment methods rather than a clear growth in absolute numbers.

## Building a Joint Understanding

Participants agreed that further work is needed to better understand the scale and drivers of money mule activity, particularly with respect to the organisers (also known as 'herders') who play a central role in money mule networks. Improving data collection, analysis and information sharing across the public and private sectors was seen as essential to developing a more accurate and comprehensive picture of the threat.

Concerns were raised about limited communication channels between NGOs, banks, platforms and public authorities. Reporting of fraudulent content was described as resource-intensive, with limited administrative capacity to address large volumes of cases.

PPPs were discussed as a means of consolidating insights across institutions. For example, the Lithuanian Centre of Excellence in Anti-Money Laundering (AML) convenes regular meetings between banks, the country's financial intelligence unit (FIU), police and other stakeholders, and publishes aggregated data on detected cases and prevented losses.

# Detection and Response

A large part of the discussion addressed measures taken by public and private stakeholders, both in Ukraine and globally, to detect and respond to money mule activity in line with AML standards and fraud controls.

## Current Efforts in Ukraine

Experts from Ukraine described measures they had taken to mitigate the risks associated with money mules, under the supervision of the National Bank of Ukraine (NBU). These measures include:

- **Risk assessment**
  During onboarding, Ukrainian banks collect identification data directly from clients and supplement it with information from external sources – including state registers, Diia (the government's digital public services platform), BankID (a bank-based electronic identification system) and data aggregators – and open source and media information, in order to form an initial risk profile. This is then combined with transaction monitoring and customer service data to assess overall customer risk. Risk assessments vary across institutions, reflecting differences in risk appetite and customer history, and this means that the same individual may be assessed differently by different banks.
- **Scenarios**
  Banks create and continuously update scenarios that may indicate a money mule, either at account opening or at a later point. The latter situation was described as more difficult to detect or anticipate since a customer who later allows their account to be used by third parties may otherwise have a low risk profile.
- **RegTech**
  RegTech solutions can be used to combine data from multiple sources (including KYC data, transaction data and device information) to detect behaviours that may be indicative of money mule activity. Several banks referred to device-based controls used alongside traditional AML monitoring, including the tracking of changes in devices and email addresses, and the continuous updating of detection scenarios.

Participants acknowledged the limitations of measures taken by banks in isolation, given that money mules can circumvent such measures by shifting their activity to a different bank. In addition, criminals operating money mule schemes often split their activities across banks to avoid detection. Two initiatives aim to mitigate this risk.

First, banks have signed a memorandum of understanding (MoU) which harmonises certain risk management practices among banks, including restrictions on card-to-card transfers. Participants noted that these limits had a tangible effect in reducing high-volume, low-value transfers; however, criminal groups have adapted by shifting transaction flows to other account types and channels.

Second, a draft law provides for the creation of a register of money mules which aims to prevent a given individual from engaging in money mule activity with multiple banks. The implementation details for the register are still under consideration – factors to consider include data protection requirements as well as the need to mitigate potential unintended consequences for innocent parties whose account or identity might have been misused without their knowledge.

Participants cautioned against overly restrictive approaches. According to one participant, every third complaint received by the NBU's consumer protection department relates to refusals to provide banking services.

# Network Analytics

International participants highlighted the importance of network analytics (the analysis of connections between individuals and entities) in the investigation of money mules.

## Benefits

Money mules are often the lowest tier in complex criminal networks. Removing individual money mules can play a part in disrupting the operations of these networks. However, if efforts are only targeted at money mules without addressing the criminal organisations that they (knowingly or unknowingly) serve, there is a risk that those organisations will continue to operate by simply recruiting other mules. Network analytics are essential to identifying herders, and should therefore be prioritised.

In addition, network analytics can help build understanding of the scale of the problem, links with predicate crimes, and the origin and destination of funds.

## Implementation

One of the international banks represented at the meeting approaches every investigation, including those related to money mules, as a network. Connections are mapped out of all available data points, including device IDs, transactions and customer behaviour.

Device IDs can help identify various patterns that are relevant to money mule detection, such as:

- The number of devices used to access a given bank account. Most customers use three to four devices (such as a computer, phone and tablet). If more than 20 device IDs are connected to the same account, this suggests that more than one individual is accessing it and therefore that it could be a money mule account.
- The number of clients per device. The same device being used to access several accounts is another risk indicator, as it might indicate that the device in question is used by a criminal group managing multiple money mule accounts.

Transactions help to identify all counterparties. Network analytics can then be used to determine who else those counterparties are interacting with, and this will often reveal a network.

Client behaviour and customer due diligence materials may reveal additional connections beyond devices and transactions.

The outcome of network analytics largely depends on the quality and comprehensiveness of the underlying dataset. This means that a network built on partial information (such as the data available to a single bank) will be less complete and will lack more connections than a network that draws on data from multiple institutions. Due to the correlation between data volume and outcome, the discussion explored ways to develop partnerships between private sector actors or between the public and private sectors.

# Unlocking the Potential of Partnerships

As outlined above, various measures have been taken in Ukraine to develop a joint response to the money mule threat, including the MoU on money mules and a potential register of fraudulent accounts. Building on these initiatives, participants identified various ways to enhance the level and impact of private–private or public–private collaboration on the detection of and response to money mules.

## Regulatory Framework

Participants recognised the importance of a regulatory framework in encouraging information sharing and discussed examples from other jurisdictions.

### The EU

Article 75 of the 2024 Anti-Money Laundering Regulation (AMLR) is the primary legal basis for private-to-private or public–private partnerships in the field of AML. The recitals of Article 75 explicitly acknowledge the key role of partnerships:

'The exchange of information among obliged entities and, where applicable, competent authorities, might increase the possibilities for detecting illicit financial flows concerning money laundering, the financing of terrorism and proceeds of crime. For that reason, obliged entities and competent authorities should be able to exchange information in the framework of an information sharing partnership where they deem such sharing to be necessary for compliance with their AML/CFT [counterterrorist financing] obligations and tasks. Information sharing should be subject to robust safeguards relating to confidentiality, data protection, use of information and criminal procedure.'

Even prior to the entry into force of Article 75, multiple EU member countries had already developed a legal basis for information sharing.

In the context of Ukraine's EU accession process, international participants encouraged Ukraine to consider how Article 75 may be implemented in the Ukrainian context.

### The UK

Different forms of information sharing are possible under UK legislation.

First, Sections 339ZB–339ZG of the Proceeds of Crime Act 2002 (POCA) provide for information sharing within the regulated sector in the context of AML efforts. The sharing may be initiated by the National Crime Agency (NCA), such as in the context of so-called 'fusion centres' like a 2024 public–private partnership aimed at identifying criminality using banking data. Staff members from participating financial institutions are seconded to these fusion centres, sworn in and granted access to the pooled data. However, once seconded to the fusion centre, they cannot relay insights directly to the bank and all communications need to be via the NCA.

Second, under the aforementioned provisions of POCA, information sharing can also be initiated by banks, under strict conditions, when the information is needed for a suspicious activity report (SAR). This sharing allows the requesting bank to gather more information and submit a more complete SAR. The information could also be used to file a joint disclosure, sometimes referred to as a 'super-SAR' – that is, a SAR

that draws on information from multiple institutions. However, joint disclosures remain rare in practice as banks are uncomfortable relying on another entity to discharge their reporting obligation.

Third, the Economic Crime and Corporate Transparency Act 2023 (ECCTA) allows for private-to-private information sharing related to all forms of economic crime. This piece of legislation disapplies civil liability as well as the General Data Protection Regulation (GDPR) if certain conditions are met (such as when both entities have a relationship with the same customer and safeguarding actions are taken to restrict the account). Information may be shared directly (Section 188) or via a third-party platform (Section 189).

## Compatibility of Information Sharing with Data Protection and Other Rules

While the potential tension with data protection and other rules was noted during the meeting discussions, various case studies were presented to demonstrate that information sharing can be done in a way that complies with those rules. Rather than legal barriers, it is often legal uncertainty that discourages private sector entities from sharing information. It was noted that the *absence of* information sharing prevents financial institutions from conducting high-quality investigations and can therefore lead to the filing of many low-quality SARs. This may in turn constitute a violation of Article 8 of the European Convention on Human Rights given the amount of personal data that these SARs reveal.

One participant emphasised the importance of regulators or FIUs issuing clear guidance on what kind of information sharing is or is not permissible. One example given was the guidance issued by the US FIU, the Financial Crimes Enforcement Network, in September 2025. The purpose of this guidance is to '(i) clarify that the Bank Secrecy Act and its implementing regulations (collectively, the "BSA") generally do not prohibit cross-border information sharing; and (ii) provide examples of information that typically would not reveal the existence of a Suspicious Activity Report (SAR) and, thus, that the BSA does not prohibit sharing.'

In the UK, guidance on the ECCTA information-sharing measures described above was issued in October 2024 by the Home Office, HM Treasury and Companies House, among other departments and agencies, and updated in October 2025. The objective of this guidance is to help regulated firms 'to utilise the new information sharing provisions introduced by sections 188 and 189'.

These two guidance documents were described as a good practice from which regulators in other countries should take inspiration. Such guidance allows banks and others to know what they can share with each other, both domestically and internationally, under applicable legislation.

## Harnessing Technology to Enable Information Sharing

In Ukraine, banks already use a digital platform to share red flags (with no personal data included) in real time. The Ukrainian Interbank Payment Systems Member Association platform enables the sharing of fraud indicators, typologies and updates on emerging signs of fraud across the banking sector.

International participants referred to technology solutions that allow for broader information sharing.

One participant described the successful use of secure channels to facilitate GDPR-compliant information sharing between banks, including across borders. The implementation of such solutions depends on multiple factors, including:

- Close coordination between all relevant teams within an institution to cover all technological, legal and operational aspects in a coherent way.
- An understanding of what can be shared in the relevant jurisdiction(s).
- A clearly defined use case (such as pooling of fraudulent account numbers, messaging between investigators from participating institutions, or joint investigations).
- A proper usage agreement between participants.
- Leadership from a small group of banks or a banking association that can test a proof of concept before securing wider adoption.

The participant shared a quote from a platform user describing how coordination between one of Scandinavia's largest banks and one of the Baltics' largest banks had stopped a mule account in time to enable the return of €100,200 to the victim of a phone scam.

Another participant pointed out the growing number of payment system operators using RegTech solutions to allow for the real-time tracing of money mule flows between payment system participants. Such tracing capabilities increase the chances of recovering funds before they are cashed out, transferred overseas or converted into virtual assets, at which point recovery becomes more difficult. Jurisdictions that have adopted tracing capabilities for fast payment systems include the UK and Malaysia.

Federated learning was mentioned as one option allowing for a joint response to money mules without requiring the sharing of personal data. While there are various implementations, federated learning generally refers to the training of a machine learning model based on distinct datasets that may be owned by different institutions. According to one participant, Article 75 of the AMLR could provide the basis for federated analysis of a customer who might have accounts with multiple institutions. For example, a third party could analyse federated data (either raw data or risk signals) from across institutions to identify patterns that may not be visible to any institution individually.

## Case Studies

Participants highlighted two PPPs coordinated by Europol.

### European Money Mule Action

Europol's European Money Mule Action (EMMA) is a cross-border PPP designed to disrupt money mule networks at scale. Between 2016 and 2024, law enforcement agencies and financial institutions from EU and non-EU countries conducted multiple coordinated operations leading to the arrest of money mules and recruiters. The impact of EMMA is the result of information sharing between all partners that allows law enforcement to identify networks and decide on the most effective disruption strategy. An EMMA operation in 2021 resulted in 1,803 arrests and the identification of over 18,000 money mules.

EMMA draws on the earlier experience of a similar public–private initiative in the Netherlands. This initiative was said to have significantly reduced the number of money mules by making the country less attractive for money muling.

### EFIPPP Money Mule Working Group

The Europol Financial Intelligence Public Private Partnership (EFIPPP) recently started a working group on money mules with participants from the public and private sectors. Private sector participants share information data on the second layer of money muling – that is, the destination of fraud proceeds after the initial transfer from the victim. Participants do not share any personal data related to the beneficiaries, but rather provide information on the financial institutions where the relevant accounts are held. Thanks to aggregated information from all members, the working group identifies banks that have higher exposure to money mule activity (and which may not be part of EFIPPP). These findings are used as a basis for engagement with the relevant banks on their vulnerabilities and the quality of their controls.

# Upstream Prevention

In addition to detection and enforcement, addressing money mule activity requires measures that operate upstream – that is, before any financial transaction is attempted. Participants discussed the role of education and financial literacy efforts, as well as of deterrence.

## Educational Measures

Education and financial literacy were identified as key preventive tools for reducing vulnerability to money mule recruitment.

Participants highlighted that limited awareness of financial crime risks, particularly among young people, increases exposure to recruitment. Banks, public authorities and law enforcement in Ukraine have therefore taken measures to inform clients about the risks and consequences of allowing their accounts to be misused, including the following:

- Banks have delivered a range of educational initiatives aimed at younger audiences, including outreach in schools and sessions with students as young as 14. This includes showing educational videos targeted at specific types of clients and providing direct advice on conditions for account use.
- The public awareness campaign #FraudstersGoodbye focuses on fraud and money mule risks associated with sharing banking details. The campaign includes interactive educational materials designed for use within the public education system, and several meeting participants noted their active uptake in practice. Importantly, this awareness campaign is implemented through partnership across the public and private sectors, including mobile service providers, public ministries, banks and private businesses.
- The Cyber Police has delivered lectures at higher education institutions as well as training sessions for prosecutors on high-tech financial crime methods.

Representatives from Ukraine stressed the importance of identifying the most effective channels for awareness-raising efforts, including channels through which recruitment occurs, such as social media and messaging platforms. It was also noted that some

groups in society may have limited trust in banks or public authorities, which can limit the effectiveness of official campaigns delivered by such institutions.

The work of the Organisation for Economic Co-operation and Development on financial literacy, in particular its report on 'The Application of Behavioural Insights to Financial Literacy and Investor Education Programmes and Initiatives', was cited as helpful in designing more effective programmes tailored to different age groups. Behavioural insights can inform the design of financial literacy initiatives by going beyond information provision to include persuasion, incentivisation and other behavioural interventions that can influence financial decision-making. Digital tools, including AI-enabled solutions, can also support more personalised messaging and allow educational content to be adapted to formats and platforms commonly used by younger audiences.

Finally, participants raised the importance of assessing the impact of education and awareness-raising interventions, including through surveys and interviews with money mules.

## Deterrence

Some participants expressed concerns about the perceived lack or low severity of criminal sentences imposed on money mules. This may weaken deterrence and contribute to the perception that individuals making their account available face few legal consequences, particularly for first-time or low-value cases.

Another factor contributing to lighter sentences is that it may be challenging in certain cases to demonstrate the required criminal intent – that is, an individual's awareness that their account would be used for criminal purposes.

Against this background, some participants argued that Article 200 of the Criminal Code of Ukraine, which addresses illegal actions involving payment instruments, should be amended to strengthen its enforceability and deterrent effect. Other participants cautioned against the unintended consequences of an approach centred on convictions of money mules. Concerns were raised about the risk of high numbers of convictions, particularly among young people, and the impact this could have on their future access to and interaction with the financial system.

# The Role of Public–Private Partnerships in Education

Participants also discussed the potential role of PPPs in delivering coordinated and effective awareness-raising communications to the public. As described earlier, the Lithuanian Centre of Excellence in AML collects data from banks; it then uses this data to support regular public communication, including press releases and sustained engagement with national television and online media to keep financial crime risks visible to the wider public.

There was a common view that, for awareness-raising campaigns to be effective, partnerships need to extend beyond banks and public authorities to also include civil society organisations and social media companies. Engaging with those additional stakeholders can help to disseminate educational materials through the channels that are most used by at-risk groups.

# Next Steps

As reflected in this report, elements of public–private cooperation already exist in Ukraine. However, the effectiveness of those efforts will depend on the willingness of stakeholders to move from ad hoc cooperation and discussions to systematic, operational and resilient partnerships as a next step.

To build such partnerships, international experts recommended building on trusted cooperation channels, possibly within a small group of institutions, and starting with narrowly defined use cases, such as tackling money mules. They also encouraged Ukrainian stakeholders to push boundaries and view a partnership as an iterative process that will require adjustments over time.

## 194 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 194 years.



RUSI is registered as a charity in England and Wales

Charity number: 210639

VAT number: GB752275038