CENTER FOR FINANCIAL INTEGRITY

CFS RUSI Centre for Finance & Security

RESEARCH BRIEFING

Money Mules in Ukraine

A Growing Threat to Financial Stability and Security

Mark Karandas and Oksana Ihnatenko

SEPTEMBER 2025

The Center for Financial Integrity

The Center for Financial Integrity (CFI), based in Chernihiv, is a non-governmental organisation committed to strengthening the resilience and integrity of Ukraine's financial system. Drawing on its expertise and convening power, CFI promotes the integration of Ukraine's financial framework with European and international standards for combating financial crime. To achieve its mission, CFI works to enhance Ukraine's financial resilience and integrity, strengthen public–private partnerships in the fight against financial crime, align Ukraine's financial crime prevention standards with those of the EU, and deepen understanding among Ukrainian stakeholders of the intersection of finance and security.

This publication is intended for general informational purposes only. Before making any decisions or refraining from action based on its content, you should seek advice from a professional or specialist adviser. The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of CFI or any other organisation. For details on terms of use, please visit CFI's website. To the fullest extent permitted by law, CFI shall not be liable for any loss or damage, whether foreseeable or not (including, but not limited to, defamation), arising from or related to the reproduction, reliance upon, or use of this publication or any information contained within it by you or any third party.

This publication was produced in cooperation with Centre for Finance and Security at RUSI.

© 2025 Center for Financial Integrity
Money Mules in Ukraine: A Growing Threat to Financial Stability and Security, September 2025

Cover image: CryptoWallet.com / CC BY 2.0

Money Mules in Ukraine: A Growing Threat to Financial Stability and Security

Introduction

Since the beginning of Russia's full-scale invasion of Ukraine, one of Kyiv's most urgent priorities has been to maintain a stable and consistent flow of revenue to the state budget. This supports national defence and essential services. At the same time, Ukraine – like many other countries – faces persistent challenges related to tax evasion and money laundering. These weaken the integrity of its financial system and make the playing field for businesses uneven.

Money mules are a widespread and damaging method used in money laundering schemes. Money mules may provide their personal banking details, identification data or bank cards to facilitate illicit financial transactions. However, it is important to recognise the different scenarios: some individuals act unwittingly, unaware that they are participating in criminal activity, while others have their accounts compromised by fraudsters, and, in some cases, participants may be fully complicit, knowingly assisting in the illegal transfers. Such schemes often involve hundreds or even thousands of participants. They create a vast and difficult-to-trace network that enables the flow of criminal funds. The consequences are severe for the state, the economy and the individuals involved. Once financial institutions detect suspicious activity, affected individuals may lose access to banking services. This can lead to long-term exclusion from the financial system, hindering their ability to receive wages, secure housing loans or conduct basic non-cash transactions – particularly problematic as Ukraine continues its shift towards a cashless economy.

Money mule networks provide an efficient, low-risk tool for criminal groups to launder and move criminal proceeds, while also financing terrorism, sabotage and some covert Russian operations. These networks contribute to increased crime and further erode state revenue – thereby weakening Ukraine's ability to finance its defence and recovery from Russia's aggression.

As such, tackling the use of money mules and dismantling the networks that enable them is an urgent and strategically important task for Ukraine.

Methodology

This briefing is informed by a review of the existing policy literature and court decisions in Ukraine, as well as grey literature that was published between 2017 and 2025 by Ukrainian and international media. The literature review is supplemented by five interviews with representatives of the public and private sectors of Ukraine's financial system, and their responses to information requests. The interviews took place between May and August 2025.

Understanding Money Mules: Definitions and Behaviour

The terms 'money mule' and 'drop' are increasingly common in discussions of financial crime. Definitions of these terms vary by country and institution.[1] The National Bank of Ukraine (NBU), the country's central bank, defines money mules as individuals who, in exchange for a fee, provide their bank-card details or identification data to third parties.[2] These accounts are then used to move or launder illicit funds, often as part of larger criminal networks.[3]

The research has identified several types of people who, depending on the context, could be money mules. Such types include those who: receive funds in their bank account and transfer them to a cybercriminal; sell control of their bank account to a cybercriminal; open a bank account for the benefit of a cybercriminal using a fake ID; pick up cash from ATM hackings or card-processing attacks; and others.[4]

Typical money mule behaviour mimics that of consumers and resembles legitimate activity. This makes it difficult to assess the true scale of money mule activity. That said, for individual cases, there may be red flags such as small test payments (for example, valued at $1) to verify stolen credentials, frequent transfers into accounts with low daily balances and rapid movement of funds. Access patterns can also raise suspicion – such as logins from high-risk countries, frequent device location changes, use of VPNs or proxies, or multiple accounts accessed from the same device or IP address. One of the specific features of Ukrainian money mules is that their transactions often resemble donations to the military, which complicates the monitoring process for banks.

In Ukraine, there were signs of increasing money mule activity. NBU data shows a consistent rise in the volume of peer-to-peer (P2P)[5] card transfers since late 2023. In 2023 alone, monthly P2P volumes grew from UAH 210 billion ($5.061 billion) in January to UAH 247 billion ($5.953 billion) in December.[6] This growth is evident across all banking groups, regardless of the size of their card-business portfolios.

The Financial Action Task Force,[7] the global standard-setter in anti-money laundering / counter-terrorist financing (AML/CTF), has identified money mules as a common tool that organised crime uses to move and conceal proceeds.[8] Internationally, individuals are often recruited through fake job adverts, online scams and coercion – highlighting the need for public awareness and preventive measures.

[1] Money mules and drops are, in essence, interchangeable concepts. Each denotes individuals who serve as intermediaries through which criminal groups channel illicit funds.

[2] National Bank of Ukraine (NBU), <https://bank.gov.ua/en/>, accessed 28 July 2025.

[3] Viktor Volokita, « У НБУ розповіли про майбутні проблеми "дропів" » ['The NBU Spoke about the Future Problems of "Drops"'], 24 May 2024, <https://epravda.com.ua/news/2024/05/24/714190/>, accessed 28 July 2025.

[4] Anton Moiseienko and Olivier Kraft, 'From Money Mules to Chain-Hopping: Targeting the Finances of Cybercrime', *RUSI Occasional Papers* (November 2018), <https://www.rusi.org/explore-our-research/publications/occasional-papers/money-mules-chain-hopping-targeting-finances-cybercrime>, accessed 15 September 2025.

[5] Instant peer-to-peer (P2P) transfer transactions are real-time electronic payments made directly between individuals, typically using bank cards, mobile apps or digital wallets.

[6] Dmytro Oliinyk, « Легкий спосіб заробітку з тяжкими наслідками або Як НБУ бореться з "дропами" » ['An Easy Way to Make Money with Serious Consequences or How the NBU Fights "Drops"'], 23 May 2024, <https://epravda.com.ua/columns/2024/05/23/714156/>, accessed 28 July 2025.

[7] The Financial Action Task Force (FATF) is an intergovernmental body that establishes standards to assist countries in combating money laundering, terrorist financing and other financial crimes. Its 40 Recommendations form a comprehensive framework that guides national authorities in identifying risks, implementing preventive measures and ensuring effective enforcement to safeguard financial and economic stability. FATF, 'What We Do', <https://www.fatf-gafi.org/en/the-fatf/what-we-do.html>, accessed 23 July 2025.

[8] FATF, 'Professional Money Laundering', July 2018, p. 27, <https://www.fatf-gafi.org/en/publications/Methodsandtrends/Professional-money-laundering.html>, accessed 28 July 2025.

Institutional Response and Criminal Adaptation

Institutional Measures

The use of money mule schemes intensified during the Covid-19 pandemic[9] and the full-scale invasion in 2022.

In response, Ukrainian law enforcement agencies (LEAs) and banks have taken steps to dismantle the networks behind these operations. Since 2022, banks have launched public awareness campaigns to warn against sharing banking data in exchange for 'easy money' – a practice that can result in criminal liability under the Criminal Code of Ukraine (CCU).

The NBU, as the sector regulator, has introduced targeted measures against money mules. Among others, it intensified penalties for non-compliance with AML and KYC requirements for banks and financial institutions.[10] On 1 October 2024, the NBU imposed a monthly transfer cap of UAH 150,000 (approximately $3,800) per individual for card-to-card transactions.[11] Following this, transaction volumes dropped from UAH 250 billion ($6.025 billion) to UAH 170 billion ($4.097 billion) per month – an early indication of impact in terms of a reduced value of payments.[12] It has also urged banks and non-bank financial institutions to deny services to individuals who cannot clearly explain the origin of their funds or justify rapid and unusual account activity.

One expert who was interviewed noted that the typical money mule holds accounts in three different Ukrainian banks. Before the introduction of the above limits and increased regulatory scrutiny, third parties could use these accounts for three to four months without detection. As a result of recent measures, this period has been significantly shortened, limiting the window for illicit activities and increasing operational/transactional costs of money mule networks.[13]

Banks, in cooperation with the banking associations, signed a memorandum to enhance transparency in the payment services market and combat money mule schemes.[14] The agreement enables information sharing on suspicious clients and activities – an effective example of public–private partnership against financial crime. In February 2025, the memorandum initiated a monthly transfer cap of UAH 50,000 (approximately $1,200) for high-risk clients.

[9] FinCEN, 'Advisory on Imposter Scams and Money Mule Schemes Related to Coronavirus Disease 2019 (COVID-19)', FinCEN Advisory FIN-2020-A003, 7 July 2020, <https://www.fincen.gov/system/files/advisory/2020-07-07/Advisory_%20Imposter_and_Money_Mule_COVID_19_508_FINAL.pdf>, accessed 15 September 2025.

[10] The NBU intensified penalties for non-compliance with AML and KYC requirements for banks and financial institutions. See NBU, Official Announcements, <https://bank.gov.ua/ua/news/all/natsionalniy-bank-u-travni-2025-roku-zastosuvav-do-dvoh-bankiv-ta-shesti-nebankivskih-finansovih-ustanov-zahodi-vplivu-za-porushennya-u-sferi-finmonitoringu-ta-valyutnogo-zakonodavstva>, accessed 15 September 2025; LigaZakon, Economic Media Coverage, <https://biz.ligazakon.net/news/236840_nbu-naklav-mlyonn-shtrafi-na-banki--fnkompan-za-porushennya-fnmontoringu>, accessed 15 September 2025.

[11] NBU, « Постанова правління Національного банку України "Про внесення змін до постанови Правління Національного банку України від 24 лютого 2022 року № 18" » ['Resolution of the Board of the National Bank of Ukraine "On Amendments to the Resolution of the Board of the National Bank of Ukraine No. 18 Dated 24 February 2022"'], 27 August 2024, <https://bank.gov.ua/ua/legislation/Resolution_27082024_102>, accessed 7 August 2025.

[12] UNN, 'Monthly Transfers after Restrictions Fell by UAH 80 Billion - NBU Announced a Register of Risky Clients', 15 April 2025, <https://unn.ua/en/news/monthly-transfers-after-restrictions-fell-by-uah-80-billion-nbu-announced-a-register-of-risky-clients>, accessed 7 August 2025.

[13] Author interview with anonymous expert A, Kyiv, 26 June 2025.

[14] NBU, « Українські банки за координації банківських асоціацій підписали Меморандум про забезпечення прозорості функціонування ринку платіжних послуг » ['Ukrainian Banks, in Coordination with Banking Associations, Have Signed a Memorandum on Ensuring Transparency in the Functioning of the Payment Services Market'], 10 December 2024, <https://bank.gov.ua/ua/news/all/ukrayinski-banki-za-koordinatsiyi-bankivskih-asotsiatsiy-pidpisali-memorandum-pro-zabezpechennya-prozorosti-funktsionuvannya-rinku-platijnih-poslug>, accessed 7 August 2025

Introduction of New Measures to Combat Money Mules

Ukrainian authorities are exploring various strategies to fight money mule schemes. In 2024, the NBU announced plans to create a money mule registry that aims to systematise banks' data on identified money mules. The specified registry will consolidate information on client identities, associated payment cards and the reporting bank. The National Police of Ukraine have also proposed criminalising money mule schemes under a separate article of the CCU.[15]

The planned 'register of money mules' or 'register of persons requiring enhanced control' will include individuals who meet specific risk criteria. Such individuals will be able to use Ukraine's financial system, but their activities will be subject to targeted restrictions currently under development by the NBU. For example, the right to change the financial phone number, be issued with new cards and top up or withdraw funds in the middle of the night will be limited. All licensed banks and financial service providers will have access to the register and will be required to apply these restrictions consistently. The tax authorities and the police will be granted access to the specified register as part of the standard disclosure of banking confidentiality. Individuals listed in the register will be aware of this and will have the right to challenge such inclusion either by appealing to the NBU or through judicial review.[16]

However, some experts question the necessity of establishing the register, noting that the existing tools within the AML/CTF framework – such as customer due diligence (CDD) procedures, transaction monitoring systems, suspicious activity reporting (SAR) mechanisms, interbank information sharing, and regulatory oversight – may already be sufficient to detect, prevent and mitigate money mule activity without introducing additional bureaucratic complexity.[17] It is essential that any such register be administered by the NBU rather than the police, in order to ensure clear separation of supervisory functions and to minimise the risk of malpractice.

The NBU, along with other state authorities, plans to implement preventive measures to tackle the phenomenon of money mules. However, the idea of criminalising money mule activities is not supported by the financial services market regulator. Such a move could negatively impact ordinary users of financial services and place an additional burden on courts, law enforcement and prosecutors – institutions already stretched by wartime demands.[18]

To cope with money mules, the authorities continue to develop enhanced tools to support banks in identifying suspicious activity and disrupting mule operations, recognising that a system-wide response is essential to address this evolving threat.

[15] Mark Savenko, « Нацполіція розробила законопроект про відповідальність дропів, - Вигівський » ['The National Police Has Developed a Bill on the Liability of Droppers'], Ukrainian News, 17 January 2025, <https://ukranews.com/ua/news/1059213-natspolitsiya-rozrobyla-zakono-proekt-pro-vidpovidalnist-dropiv-vygivskyj>, accessed 28 July 2025.

[16] Author interview with anonymous expert A, Kyiv, 26 June 2025.

[17] Author interview with anonymous expert C, online, 7 August 2025.

[18] Author interview with anonymous expert A, Kyiv, 26 June 2025.

Evolving Tactics by Criminal Networks

Criminal actors are now adapting their tactics to avoid quick detection.

To mimic legitimate behaviour and reduce suspicion, they now conduct transactions typical of everyday life – such as purchasing groceries or household items, paying utility bills and engaging in online shopping – through these accounts.[19]

As a part of their efforts to detect the money mule activities, banks routinely analyse financial transactions and contact account holders for verification. In response, the organisers behind money mule networks have developed sophisticated countermeasures. These criminal groups recruit 'actors' to impersonate the actual account holders. They use specialised software to superimpose the real money mule's photos or videos on to the actor's face during video calls with bank representatives. In addition, these networks increasingly rely on AI to forge convincing documents – such as bank statements, deposit certificates and tax returns. The high quality of these AI-generated documents makes them difficult to distinguish from authentic ones, significantly restricting the ability of banks to verify customer identities and detect suspicious activity.[20]

Another tactic involves the growing use of virtual assets in money mule schemes, which are becoming increasingly organised and decentralised. At the beginning of the full-scale invasion, the NBU imposed temporary restrictions on international wire transfers to prevent large-scale capital flight and stabilise the national economy, while the use of virtual assets surged in response. Some experts estimate that crypto-related mule operations cost the Ukrainian budget about UAH 1 billion (about $24 million) per month.[21]

Economic and Social Impact in Ukraine

The widespread use of money mules in Ukraine poses serious risks to the national economy, the financial system and social stability. These schemes both undermine public revenues and lead to long-term exclusion of individuals from essential financial services. The impact on individuals has broader implications for employment, social welfare and economic development.

Impact on Individuals

Individuals involved, knowingly or not, often face permanent or long-term exclusion from the financial system. Once flagged by multiple banks, they may be unable to receive salaries, obtain loans or open business accounts. Even though procedures exist for re-establishing banking relationships, they are rarely used, are complex and require detailed financial disclosure. The lack of financial access significantly limits a person's ability to participate in the modern cashless economy, compounding personal and professional setbacks.

[19] Author interview with anonymous expert B, Kyiv, 11 July 2025.

[20] *Ibid.*

[21] Oksana Ihnatenko and Greta Barkauskienė, 'Public–Private Partnerships and Virtual Assets in Ukraine: Taskforce Report', RUSI, August 2025, <https://www.rusi.org/explore-our-research/publications/conference-reports/public-private-partnerships-and-virtual-assets-ukraine-task-force-report>, accessed 15 September 2025.

Economic Impact

Money mule activity results in substantial losses to the state budget. According to the NBU and members of parliament, over UAH 200 billion ($4.82 billion) annually flows through these schemes, with potential tax losses reaching UAH 50 billion ($1.25 billion).[22] This undermines the state's capacity to fund social programmes and invest in development: the mules conceal taxable income and facilitate the shadow economy.

Banks, in turn, are forced to sever relationships with suspected mule clients, reducing their customer base and revenue. Furthermore, individuals with criminal records related to these schemes face long-term barriers to employment, exacerbating labour shortages. Such shortages are particularly acute due to displacement and wartime conditions.

Social Impact

Money mules are recruited from diverse demographics, including youth. These younger persons may face early legal consequences and long-term financial hardship. In many cases, third parties use mule cards to obtain credit, which is later defaulted on – leaving cardholders responsible for the debt. This leads to rising numbers of bankruptcies and debtors, increasing financial vulnerability across the population.

The ease of becoming involved – often without fully understanding the consequences – makes this a widespread social risk with systemic implications.

Legal Framework and Enforcement

As in many countries, Ukraine's legal framework does not yet contain a dedicated provision that specifically defines or penalises the actions of money mules.

Instead, LEAs assess and prosecute such individuals based on the consequences of the use of their bank cards and accounts. For example, if a money mule's card was involved in fraudulent activity, the person may face charges under Article 190 of the CCU, covering fraud.[23] In other cases, money mules are prosecuted for aiding and abetting tax evasion (Article 212 of the CCU), or for laundering the proceeds of crime (Article 209 of the CCU).

Trends in Criminal Prosecution of Money Mule Activity

The two recent examples from the Unified State Register of Court Decisions reveal cases of individuals who have been prosecuted for aiding and abetting in the fraudulent appropriation of property by deception.[24] Such cases often involve organised groups acting in collusion and using electronic means to carry out illegal financial operations.

A verdict issued by the Kyiv District Court of Poltava (case No. 552/7561/24),[25] illustrates a typical money mule operation (see Box 1).

[22] Financial Club, « Через «дропів» проходить мінімум 200 млрд грн щорічно » ['At Least 200 Billion UAH Passes Through the "Drops" Annually'], 13 August 2024, <https://www.finclub.net/news/cherez-dropiv-prokhodyt-minimum-200-mlrd-hrn-shchorichno.html>, accessed 28 July 2025.

[23] « Кримінальний кодекс України » ['Criminal Code of Ukraine: Law of Ukraine No. 2341-III of April 5, 2001'], 2001, <https://zakon.rada.gov.ua/laws/show/2341-14/conv#n1263>, accessed 7 July 2025.

[24] « Кримінальний кодекс України » ['Criminal Code of Ukraine: Law of Ukraine No. 2341-III of April 5, 2001. Article 190. Fraud'], 2001, <https://zakon.rada.gov.ua/laws/show/2341-14/conv#n1263>, accessed 7 August 2025.

[25] « Вирок Київського районного суду м. Полтави у справі No. 552/7561/24 » ['Ruling of the Shevchenkivskyi District Court of Kyiv, Case No. 552/7561/24 (Court Registry No. 123513283)'], 2024, <https://reyestr.court.gov.ua/Review/123513283>, accessed 7 August 2025.

Box 1: Money Mules and Fraud: Case No. 552/7561/24

In this case, the defendant and several accomplices were responsible for receiving funds obtained through fraud and then carrying out further transactions to distribute these funds. The fraudsters employed sophisticated methods to obscure the origin of the stolen funds, including multiple transfers between bank accounts and the involvement of numerous accomplices to conceal the source and final destination of the money.

The scheme was highly coordinated: one participant was recruited by a close acquaintance, who in turn operated under the direction of an unidentified organiser. Others joined the operation through mutual contacts, creating a web of individuals who acted separately but followed a common set of instructions. Participants of the scheme used both personal and purchased bank cards to receive funds from victims and then subsequently transfer and distribute them further down the chain.

In addition to being charged with aiding and abetting fraud, individuals involved in such schemes may also face charges related to money laundering. In practice, funds are transferred to the accounts of drops who then withdraw illegally obtained funds in cash or purchase consumer goods (predominantly for their own consumption). These goods or funds are then passed on to third parties – typically the organisers or controllers of the money mule network – further distancing the core perpetrators from the financial trail.

Box 2: Money Mules and Money Laundering: Case No. 334/4002/23

The verdict of the Leninsky District Court of Zaporizhia (case No. 334/4002/23)[26] highlights how participants of money mule schemes engage in money laundering. In this case, the defendant used a bank card registered to another person, to which he had full access via a mobile banking app. The defendant received UAH 15,000 ($310), knowing the funds were obtained through fraud. To conceal the origin of these funds and make the transactions appear legitimate, he transferred UAH 10,000 ($207) to another card, also issued in a third party's name. In this way, the defendant legalised funds totalling UAH 10,000 ($207).

Legal entities can also play a role in schemes involving money mules and may bear responsibility under applicable criminal provisions. Businesses sometimes use drop accounts to avoid declaring revenue and paying taxes. For example, when a customer purchases consumer goods, payment may be made not to the official account of the legal entity selling the goods, but instead to that of a money mule. The mule then withdraws the money in cash or transfers it to other drop accounts, effectively concealing the income from tax authorities.

In Ukraine, the prosecution of money mules is still relatively rare. A key challenge is that charges are typically filed only when a mule's account can be explicitly tied to a serious, indictable offence such as money laundering, drug trafficking or tax evasion. For a conviction to happen, law enforcement must successfully prove that the mule's account was a component of a larger criminal plot orchestrated by others. This highlights the gap between identifying misuse and securing a criminal conviction.

[26] « Вирок Ленінського районного суду м. Запоріжжя у справі No. 334/4002/23 » ['Verdict of the Leninskyi District Court of Zaporizhzhia, Case No. 334/4002/23'], 2023, <https://reyestr.court.gov.ua/Review/112356393>, accessed 7 August 2025.

International Practices

Money mule schemes pose a global threat. Many countries are implementing targeted measures to combat their use in money laundering, with varying levels of success.

In the UK, the Financial Conduct Authority (FCA), as reported by the *Financial Times*, identified more than 200,000 individuals as money mules in the past year alone – an alarming figure that illustrates the rapidly increasing prevalence of money mule activity.[27]

Criminals in the UK are increasingly funnelling illicit funds through digital banks, small payment firms and banking-as-a-service providers, which often have weaker onboarding and compliance controls.[28] These newer institutions receive a disproportionately high share of fraudulent transactions compared with their overall market activity, suggesting that they are attractive targets.

The data from financial institutions such as Santander UK PLC and Barclays PLC indicates that younger individuals, especially those aged under 30, are more susceptible to becoming money mules, often due to financial pressures and the allure of easy money.[29] The consequences of acting as a money mule in the UK are serious and far-reaching, including criminal prosecution, substantial fines, imprisonment and lasting damage to one's financial reputation and career prospects, as individuals may also be recorded in the CIFAS fraud prevention database, which can affect future banking relationships and professional opportunities.

In Poland, money mule operations often involve the use of foreign identity documents, deliberately complicating the verification of document authenticity and account holder legitimacy. To counter this, the Polish Bank Association (ZBP)[30] operates several databases that contain information on fraudulent bank accounts and their holders – in most cases, individuals acting as money mules.[31]

Public awareness and education are central to Poland's anti-money mule strategy, serving as a critical first line of defence and offering a useful model for Ukraine's efforts. National efforts are reinforced by participation in EU-wide initiatives such as #Don'tBeAMule and European Money Mule Action Weeks (EMMA Weeks).[32] Such efforts have been effective in raising public awareness, preventing mule account misuse and complementing broader enforcement efforts across the financial sector.

Polish experts highlight several key challenges in tackling money mule networks: the speed and anonymity of digital transactions hinder real-time fund tracing, while the global nature of these schemes complicates cross-border coordination.[33] Financial institutions must also balance effective compliance with maintaining user trust. Strengthening international cooperation, data sharing and public awareness remains essential to counter these evolving threats.

[27] Martin Arnold, 'Surge in "Money Mules" Raises Concern at UK Financial Watchdog', *Financial Times*, 13 August 2025.

[28] Kathryn Westmore and Allison Owen, 'Following the Fraud: The Role of Money Mules', RUSI Emerging Insights, August 2025, <https://www.rusi.org/explore-our-research/publications/emerging-insights/following-fraud-role-money-mules>, accessed 15 August 2025.

[29] Fintech Global, 'Understanding the Role of Money Mules in Financial Crime and Fraud Prevention', 3 April 2025, <https://fintech.global/2025/04/03/understanding-the-role-of-money-mules-in-financial-crime-and-fraud-prevention/>, accessed 28 July 2025.

[30] Polish Bank Association (ZBP), <https://www.zbp.pl/?lang=en-us>, accessed 31 July 2025.

[31] Author interview with anonymous expert D, online, 4 July 2025.

[32] The European Money Mule Action Weeks (EMMA Weeks) are coordinated law enforcement campaigns led by Europol and national agencies across Europe to target money mule networks.

[33] Author interview with anonymous expert D, online, 4 July 2025.

In the US, individuals from diverse backgrounds are involved in such schemes. The FBI places money mules into one of three categories: unwitting or unknowing money mules are unaware that they are part of a larger scheme; witting money mules ignore obvious red flags or their money movement activity; and complicit money mules are aware of their role and actively participate.[34]

To combat this issue, the US Department of Justice coordinates the Money Mule Initiative, an annual nationwide effort involving multiple federal agencies, including the FBI, IRS Criminal Investigation and the Postal Inspection Service. The initiative focuses on identifying and disrupting mule networks, raising public awareness, and pursuing enforcement actions.[35] It unites the efforts of various federal institutions in the fight against money mule schemes. Furthermore, under Section 314(b) of the PATRIOT Act, financial institutions are permitted and encouraged to share information with one another. This legal provision supports cross-institutional coordination, allowing for faster identification of money mule networks and improved disruption of illicit financial flows.

Conclusion

Money mule schemes pose a significant threat to Ukraine's financial stability, social cohesion and state revenue. Addressing this issue requires state authorities and other stakeholders to be proactive and coordinate their response. Such efforts should focus on public awareness campaigns, practical examples of legal consequences and strengthened preventive measures.

Current detection systems often identify mule activity only following substantial transactions. This highlights the need for earlier intervention and real-time monitoring tools. Ukraine's recent restrictions on card-to-card transfers have shown promise and could serve as a key lever in curbing illicit flows.

International experience shows that money mules are a growing problem worldwide, requiring targeted regulation, public education and cross-sector cooperation and public–private partnerships to significantly reduce the scale and impact of money mule networks.

About the Authors

Mark Karandas is an Associate Fellow at the Center for Financial Integrity. He is a seasoned professional with practical experience in both national and international financial institutions, including an internship at the NBU and roles in commercial banking.

Oksana Ihnatenko is the Managing Director of the Center for Financial Integrity. She is also a Researcher on Ukraine's financial integrity in RUSI's Centre for Finance and Security. Her research examines the resilience and integrity of Ukraine's financial system. Oksana is a Certified Anti-Money Laundering Specialist.

[34] FBI, 'Money Mules', <https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/money-mules>, accessed 28 July 2025.

[35] US Department of Justice, 'Justice Department Announces Landmark Money Mule Initiative', 4 December 2019, <https://www.justice.gov/archives/opa/pr/justice-department-announces-landmark-money-mule-initiative>, accessed 28 July 2025.