https://www.proconference.org/index.php/usc/article/view/usc33-00-038
DOI: 10.30888/2709-2267.2025-33-00-038

UDC 004.2

ADMINISTRATIVE-LEGAL REGULATION OF ANTI-MONEY LAUNDERING DURING MARTIAL LAW IN UKRAINE

Holota N.P.
c.j.s., as.prof.
ORCID: 0000-0003-4113-7743
Vinnytsia Educational and Scientific Institute of Economics of West Ukrainian National University, Vinnytsia, Ghonty, 37, 21017

Abstract. *This study examines the primary challenges of anti-money laundering (AML) systems during armed conflicts, utilizing Ukraine's experience following the Russian invasion on February 24, 2022, as a case study. It demonstrates that traditional AML mechanisms, designed for peacetime conditions, are ineffective in wartime due to mass population displacement, infrastructure destruction, and the urgent need to mobilize resources. The research reveals new money laundering typologies linked to the misuse of humanitarian aid, corruption in defense procurement, and exploitation of refugee status. It proposes amendments to AML legislation, including simplified identification procedures for displa ced persons, extended compliance deadlines under force majeure, and exemptions from administrative liability during hostilities. The paper concludes that a specialized AML regime is required to reflect wartime realities while balancing national security needs, international obligations, and citizens' rights.*

Keywords: *anti-money laundering, financial monitoring, martial law, armed conflict, sanctions, suspicious transactions, administrative liability, virtual assets, humanitarian aid, internally displaced persons, force majeure circumstances.*

Introduction.

The problem of anti-money laundering (AML) in the context of armed conflicts represents one of the most complex areas of modern law. A full-scale war not only destroys the economic infrastructure of the state but also creates a unique legal and factual environment in which traditional mechanisms of combating the legalization of criminal proceeds prove to be insufficiently effective or require fundamental reconsideration. The significance of this matter has gained particular urgency for Ukraine with the beginning of the full-scale Russian aggression on February 24, 2022. Martial law, mass population migration, the destruction of banking infrastructure, the escalation of humanitarian initiatives, along with the imperative to mobilize comprehensive resources for national defense, have established an entirely new operational framework for the financial system. Within this context, novel risks and vulnerabilities related to money laundering have surfaced, demanding both conceptual analysis and actionable responses through national and international legal mechanisms.

The traditional AML system, built on the basis of the recommendations of the Financial Action Task Force (FATF) [1] and implemented through national legislation, has proven unprepared for the challenges of wartime. Standard procedures of client identification, financial transaction monitoring, and suspicious transaction reporting require adaptation to the realities of armed conflict. At the same time, the war creates new channels for money laundering related to corruption in defense procurement, abuses of humanitarian aid, and the use of refugees for financial operations, among others.

Main text.

The system of combating the legalization (laundering) of proceeds of crime in Ukraine is regulated by the Law of Ukraine of December 6, 2019, No. 361-IX "On Prevention and Counteraction to Legalization (Laundering) of Proceeds from Crime, Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction" [2] and subordinate regulatory acts. Article 12 of this Law establishes mandatory client identification procedures, which, under martial law, face objective obstacles. Mass population migration, the loss of documents during bombardments, and the destruction of civil registry offices create situations in which citizens cannot provide a complete set of documents for proper verification.

The introduction of martial law based on the Decree of the President of Ukraine of February 24, 2022, No. 64/2022 "On the Introduction of Martial Law in Ukraine" [3] created legal grounds for restricting certain constitutional rights and freedoms in accordance with Article 64 of the Constitution of Ukraine [4]. Resolution of the National Bank of Ukraine (NBU) No. 95 of June 18, 2020, "On Approval of the Regulation on the Organization of the Risk Management System in Banks of Ukraine and Banking Groups" [5] requires banks to verify client information through independent sources.

In wartime, a significant part of the state registers located in the occupied territories is inaccessible, and documents originating from these territories may have questionable authenticity. This creates legal uncertainty regarding the possibility of servicing internally displaced persons and refugees. The identification of legal entities

whose founders or beneficial owners are located in the occupied territories becomes particularly complex. The inability to obtain up-to-date documents or confirm information about such persons creates risks both for banks (potential fines for improper due diligence) and for clients (denial of service).

Under martial law circumstances, new typologies of financial operations emerge that require special attention from the AML system. Operations involving money transfers for the procurement of weapons and military equipment, charitable contributions for army needs, and humanitarian aid have characteristics that could be qualified as suspicious under peacetime conditions. NBU Resolution No. 65 of 28.04.2020 “On Approval of the Regulation on Financial Monitoring by Banks” [6] contains a list of suspicious operation indicators that is not adapted to wartime realities. Particularly, cash operations exceeding established thresholds in frontline regions may be related to the inability to use electronic payments due to infrastructure damage, rather than to intentions of money laundering. At the same time, new money laundering schemes specific to wartime emerge: the use of charitable funds for legitimizing criminal proceeds, corruption schemes in defense procurement, and abuse of refugee status for financial operations. These schemes require the development of new detection criteria and special investigation procedures.

Martial law is accompanied by large-scale implementation of sanctions, which fundamentally changes the tasks of the AML system. Constant updating of sanctions lists, the need to identify beneficial owners of sanctioned persons, and detection of attempts to circumvent sanctions through nominee persons create new legal and technical challenges. The application of “secondary sanctions” becomes particularly complex when Ukrainian banks may be disconnected from international payment systems for cooperation with sanctioned persons. This creates a legal collision between national interests (servicing all citizens) and international requirements (compliance with sanctions regimes). Banks are forced to simultaneously comply with the sanctions requirements of different jurisdictions – Ukraine, EU, USA, Great Britain, and other countries, which may contradict each other or have different application criteria. The absence of clear clarifications regarding the priority of different sanctions regimes

creates risks of legal errors.

Article 19 of the Ukrainian Law "On Prevention and Counteraction to Legalization (Laundering) of Proceeds from Crime, Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction" [2] establishes a thirty-day deadline for submitting reports on suspicious transactions to the State Financial Monitoring Service of Ukraine (SFMS). Under wartime conditions, banks face objective obstacles in meeting these deadlines: staff evacuation, cyberattacks, IT infrastructure damage, and power outages. Moreover, cyberattacks on the banking system can lead to the loss of information about financial transactions or the inability to access monitoring systems. This creates situations where a bank is physically unable to fulfill its financial monitoring obligations but remains formally liable for violations. The issue of preserving and transmitting information about financial transactions by banks evacuating from combat zones becomes particularly problematic. The need to ensure continuity of financial monitoring conflicts with the requirements of staff physical security and infrastructure preservation.

The Ukrainian Law No. 2074-IX "On Virtual Assets" dated February 17, 2022 [7] came into effect at the height of the war, creating additional complications for its implementation. Cryptocurrencies are actively used both for legitimate purposes (collecting donations for the army, humanitarian aid) and for illegal activities (terrorism financing, sanctions evasion). The technical characteristics of cryptocurrencies – pseudonymity, cross-border nature, and transaction irreversibility – complicate the application of traditional financial monitoring methods [8]. Tracking crypto-asset movements requires specialized technological solutions and staff training, which is problematic under martial law conditions. International coordination in the field of crypto-operations monitoring is also complicated due to different countries' approaches to virtual asset regulation and the absence of unified standards for information exchange between crypto-providers of different jurisdictions [9].

In the current conditions of armed conflicts, the problem of proportionality of administrative liability becomes relevant. In particular, the application of Article 166-9 of the Code of Ukraine on Administrative Offenses (CUoAO) [10] under martial law

creates a problem of proportionality between sanctions and the real capabilities of financial monitoring entities. Penalties for violations of AML requirements may be applied to banks that objectively could not comply with these requirements due to military actions. The absence of special provisions in the CUoAO regarding exemption from liability in connection with martial law creates legal uncertainty. References to Article 21 of the CUoAO (legal incapacity) [10] are not always applicable to force majeure situations in the activities of legal entities. Courts are forced to independently interpret the concept of "force majeure" in the context of military actions, which leads to inconsistent judicial practice and violates the principle of legal certainty.

Analysis of the identified problems indicates the need for systemic changes to anti-money laundering legislation. It would be advisable to supplement the Law of Ukraine “On Prevention and Counteraction to Legalization (Laundering) of Proceeds from Crime, Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction” [2] and subordinate regulatory acts with a separate section “Peculiarities of Application during Martial Law” which would regulate:

– simplified identification procedures for internally displaced persons and refugees;
– extended deadlines for fulfilling obligations of financial monitoring entities under force majeure circumstances;
– criteria for exemption from liability in connection with military actions;
– special requirements for operations involving humanitarian aid and charitable contributions.

We consider it advisable to develop a special subordinate act “Typologies of Suspicious Operations during Wartime” which would contain indicators for detecting money laundering schemes specific to armed conflict. It is also advisable to create legal mechanisms for temporary simplification of AML procedures for critically important operations (defense procurement, humanitarian aid) while simultaneously strengthening post-control after the end of martial law.

Conclusions.

Martial law creates systemic legal conflicts in the functioning of the anti-money

laundering system that cannot be resolved within the existing regulatory framework. The need to balance national security requirements, international obligations, and citizens' rights necessitates the development of a special AML legal regime for armed conflict conditions. The key areas of legal changes should include: adaptation of identification procedures to wartime realities, development of new typologies of suspicious operations, regulation of administrative liability issues under force majeure circumstances, and creation of mechanisms for effective international cooperation during wartime.

References:

1. FATF Recommendations. FATF. URL : ttps://www.fatf-gafi.org/en/topics/fatf-recommendations.html

2. Law of Ukraine "On Prevention and Counteraction to Legalization (Laundering) of Proceeds from Crime, Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction" No. 361-IX of December 6, 2019. URL : https://zakon.rada.gov.ua/laws/show/361-20#Text [in Ukrainian].

3. Decree of the President of Ukraine "On the Imposition of Martial Law in Ukraine" No. 64/2022 of February 24, 2022. URL : https://www.president.gov.ua/documents/642022-41397 [in Ukrainian].

4. Constitution of Ukraine: Law of Ukraine No. 254k/96-VR of June 28, 1996. Legislation of Ukraine. URL : https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80 [in Ukrainian].

5. Resolution of the Board of the National Bank of Ukraine "On Approval of the Regulation on the Organization of the Risk Management System in Banks of Ukraine and Banking Groups" No. 64 of June 11, 2018. URL : https://zakon.rada.gov.ua/laws/show/v0064500-18#Text [in Ukrainian].

6. Resolution of the Board of the National Bank of Ukraine "On Approval of the Regulation on the Implementation of Financial Monitoring by Banks" No. 65 of May 9, 2020. URL : https://zakon.rada.gov.ua/laws/show/v0065500-20#Text [in Ukrainian].

7. Law of Ukraine "On Virtual Assets" No. 2074-IX of February 17, 2022.

Legislation of Ukraine. URL : https://zakon.rada.gov.ua/laws/show/2074-20#Text [in Ukrainian].

8. Kovalchuk, O., Shevchuk, R., & Banakh, S. Cryptocurrency Crime Risks Modeling: Environment, E-Commerce, and Cybersecurity Issue. *IEEE Access*. 2024. Vol. 12. P. 50673–50688.

9. Kovalchuk O. Digital jurisprudence: the legal field of cryptocurrencies. Legal Economic Science and Praxis. 2023. Vol. 9. P. 13–17.

10. Code of Ukraine on Administrative Offenses: Law of Ukraine No. 8073-X of December 7, 1984. Legislation of Ukraine. URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text [in Ukrainian].

sent: 15.09.2025