Visegrad Fund

The project is co-financed by the Governments of Czechia, Hungary, Poland and Slovakia through Visegrad Grants from International Visegrad Fund. The mission of the fund is to advance ideas for sustainable regional cooperation in Central Europe

Modern Tools for Fraud Detection: Insights from the V4 and Ukraine

edited by
Iryna Chuy, Vilmos Lakatos and Piotr Luty

Publishing House of Wroclaw University of Economics and Business

Visegrad Fund

The project is co-financed by the Governments of Czechia, Hungary, Poland and Slovakia through Visegrad Grants from International Visegrad Fund. The mission of the fund is to advance ideas for sustainable regional cooperation in Central Europe

Modern Tools for Fraud Detection: Insights from the V4 and Ukraine

edited by
Iryna Chuy, Vilmos Lakatos and Piotr Luty

Publishing House of Wroclaw University of Economics and Business
Wroclaw 2025

Reviewer
Renáta Pakšiová

Copyediting
Elżbieta Macauley, Tim Macauley, Agnieszka Flasińska

Proofreading
Marcin Orszulak

Typesetting
Małgorzata Myszkowska

Cover design
Beata Dębska

ISBN 978-83-68394-40-5

DOI: 10.15611/2025.40.5

Quote as: Chuy, I., Lakatos, V., & Luty, P. (Eds.). (2025). *Modern Tools for Fraud Detection: Insights from the V4 and Ukraine*. Publishing House of Wroclaw University of Economics and Business.

70 LAT WYDAWNICTWA
UNIWERSYTETU EKONOMICZNEGO
WE WROCŁAWIU
1955-2025

Contents

Foreword

Fraud remains one of the most persistent challenges in modern economies, undermining financial stability, eroding public trust, and creating significant economic losses for governments, businesses, and individuals. As fraud schemes evolve in complexity, traditional detection methods struggle to keep pace. The need for innovative, data-driven approaches has never been greater. This book explores modern tools and strategies for fraud detection, with a particular focus on insights from the Visegrad Group (V4) countries – Poland, Czechia, Hungary, and Slovakia – and Ukraine.

The economic and political landscape of Central and Eastern Europe presents unique challenges for fraud detection and prevention. Countries in this region face issues such as tax evasion, occupational fraud, creative accounting, and corruption, which threaten economic development and financial integrity. Despite ongoing efforts by governments and international institutions to enhance transparency, the effectiveness of anti-fraud measures varies significantly across jurisdictions. This book highlights the lessons learned from the V4 countries and Ukraine, offering a comparative perspective on regulatory frameworks, enforcement mechanisms, and technological advancements in fraud detection.

Each chapter examines a specific aspect of fraud detection, offering theoretical insights, empirical research and case studies that illustrate both the challenges and best practices in combating fraudulent activities.

Chapter 1 explores the role of artificial intelligence (AI) in tax fraud detection. Traditional tax enforcement methods often lag behind sophisticated tax evasion tactics, but AI-driven solutions are increasingly being adopted to analyse vast datasets, identify anomalies, and predict fraudulent behaviour. The chapter highlights best practices from European tax authorities whilst considering Ukraine's unique tax fraud landscape.

Chapter 2 investigates tax security and its vulnerabilities. It presents key indicators of tax security, including fiscal burden, tax collection efficiency, and the shadow economy's impact. By analysing data from Ukrainian and international sources, the chapter offers recommendations on strengthening tax security through improved administration and enforcement.

Chapter 3 focuses on occupational fraud, a major issue affecting both private and public sectors. Employee fraud can be individual or organised, leading to significant financial and reputational damage. Using data from Transparency International and the Association of Certified Fraud Examiners (ACFE), the chapter provides an in-depth analysis of fraud trends in the V4 region and Ukraine, highlighting the importance of internal controls and digital solutions.

Chapter 4 scrutinises creative accounting practices, a deceitful technique used by businesses to manipulate financial statements. The chapter discusses the motivations behind these practices, detection models, and regulatory measures designed to mitigate financial misrepresentation.

Chapter 5 studies Ukraine's regulatory framework, the war's effects on financial reporting, and the barriers to achieving accounting transparency. It also provides recommendations for overcoming these obstacles through reforms, regulatory improvements, and professional development.

Chapter 6 addresses the controversial issue of bank account blocking by tax authorities. In many countries, tax administrations have the power to freeze accounts suspected of fraudulent activity. While intended to combat tax evasion, these measures often raise concerns regarding legal safeguards and economic impact.

Chapters 7 and 8 explore VAT fraud, particularly carousel fraud, one of the most damaging types of tax fraud in the EU. These chapters analyse how fraudsters exploit weaknesses in VAT systems, the impact of fraud on public finances, and the effectiveness of countermeasures. Real-world cases and international cooperation efforts are discussed to illustrate both successes and ongoing challenges.

Chapter 9 shifts the focus to corporate anti-corruption efforts through non-financial reporting. Businesses today are increasingly required to disclose their anti-corruption measures, reflecting a growing emphasis on transparency and ethical governance. This chapter analyses the reporting practices of Polish listed companies and assesses the role of corporate accountability in fraud prevention.

Chapter 10 provides recommendations for fighting corruption, CIT fraud, PIT fraud, VAT fraud, money laundering and using AI and modern tools for preventing fraud. The chapter sums up research and practices introduced during the project implementation.

By bringing together academic research, policy analysis, and real-world case studies, this book aims to bridge the gap between theory and practice in fraud detection. It provides valuable insights for policymakers, financial professionals, law enforcement agencies, and researchers seeking to enhance fraud prevention strategies. The lessons learned from the V4 countries and Ukraine offer broader implications for other economies grappling with similar fraud-related challenges.

Fraud is a constantly evolving threat, and combating it requires collaboration, technological innovation, and a commitment to transparency. This book serves as a resource for understanding modern fraud detection mechanisms and highlights the importance of adapting regulatory and technological solutions to an increasingly complex financial landscape.

Chapter 1

Artificial Intelligence in Tax Fraud Detection and Prevention

Vasyl Erastov

Taras Shevchenko National University of Kyiv
ORCID: 0000-0001-5230-0273

Mariia Balytska

Taras Shevchenko National University of Kyiv
ORCID: 0000-0002-7129-4232

Quote as: Erastov, V., & Balytska, M. (2025). Artificial Intelligence in Tax Fraud Detection and Prevention. In I. Chuy, P. Luty, V. Lakatos (Eds.), *Modern Tools for Fraud Detection: Insights from the V4 and Ukraine* (pp. 8-19). Publishing House of Wroclaw University of Economics and Business.

DOI: 10.15611/2025.40.5.01

1.1. Introduction

Tax fraud remains a significant challenge for governments worldwide, contributing to an estimated 4% to 15% of the tax gap in various OECD countries (Gaie, 2023). These losses place additional pressure on public finances, especially in times of economic uncertainty and high government deficits. Addressing this issue requires effective detection mechanisms that can identify fraudulent activities while minimising disruptions to legitimate taxpayers.

Traditional tax fraud detection methods rely on audits, risk assessment models, and rule-based systems. While these approaches have proven useful, they often struggle with scalability, adaptability, and the ability to detect complex fraudulent schemes. Fraudsters continuously evolve their tactics, exploiting regulatory loopholes and technological vulnerabilities, which makes manual and rule-based detection increasingly inadequate.

Recent artificial intelligence (AI) advancements offer new possibilities for enhancing tax fraud detection. Machine learning algorithms, predictive analytics, and anomaly detection techniques allow tax authorities to analyse vast datasets more efficiently, identify hidden patterns, and improve fraud prediction accuracy. Despite these promising developments, AI-driven solutions also face challenges related to data privacy, transparency, and the risk of bias, necessitating a balanced approach to their implementation.

1.2. Techniques of Tax Avoidance and Evasion

Tax avoidance and tax evasion are common problems worldwide. Their scale largely depends on the level of economic development, legislation, and corporate culture. Various theories explain this phenomenon from different perspectives, but the key interest lies not in the causes themselves, but in the implications and consequences.

AI as a set of appropriate tools cannot affect unfair taxpayer attitudes towards taxation, but it can highlight and predict such violations among other taxpayers' data. To highlight possible AI tools for tax fraud detection, it is necessary to investigate the main tax avoidance and tax evasion techniques.

Tax avoidance and tax evasion techniques are mostly common worldwide, but some countries have their own approaches. The most used tax fraud techniques are:

- Manipulating income recognition. Companies adjust the timing of income recognition to shift taxable income across different periods, lowering their tax liabilities. This is done by either delaying income recognition or accelerating expenses.
- Using tax havens and offshore subsidiaries. Companies expand their operations into low--tax jurisdictions (such as Singapore and Mauritius, as observed in the case of PT Adaro Energy) to report income in countries with lower tax rates, thereby reducing tax obligations in their home country.
- Leveraging capital intensity. Firms with high capital intensity (large investments in fixed assets) benefit from higher depreciation deductions, reducing taxable income. Since depreciation is a non-cash expense, it allows businesses to minimise tax payments while maintaining financial flexibility.
- Profit shifting through transfer pricing. Multinational firms use transfer pricing strategies to allocate profits to divisions located in low-tax countries, thus minimising taxable income in high-tax jurisdictions.
- Debt financing (thin capitalisation). Companies with high leverage can deduct interest expenses from taxable income, lowering their effective tax rates. This strategy aligns with the trade-off theory, where firms optimise debt levels to maximise tax benefits while balancing financial risks.
- Institutional ownership influence. Although institutional ownership could theoretically reduce opportunistic tax behaviour, the study found no significant correlation between institutional ownership and tax avoidance, suggesting that even well-monitored firms engage in tax planning (Cahyaningrum & Wulandari, 2024).

When addressing Ukrainian realities, there are several common tax avoidance techniques, but some of them are less common in other countries. The most common for Ukraine are the following (Institute of Social and Economic Transformation, 2024).

- Customs violations and smuggling
  - underreporting the customs value of goods to reduce import duties,
  - interrupted transit schemes, where goods are declared as transit but end up in the domestic market tax free,
  - use of intermediaries, individuals who import small quantities to avoid taxation.
- VAT fraud and manipulation
  - illegal VAT refunds through fake exports,

  - ‘mMissing trader’ and carousel schemes, where companies claim VAT refunds without real transactions,
  - product substitution, where expensive taxed products are swapped for lower-taxed ones.

- Profit shifting and offshore tax havens
  - using low-tax jurisdictions to shift profits and reduce tax obligations,
  - round-tripping, where Ukrainian-owned capital is routed abroad and reinvested as foreign investment to gain tax benefits,
  - misusing tax treaties (‘treaty shopping’) to take advantage of preferential tax rates.

- Shadow economy and unregistered business activities
  - unreported cash transactions in retail and services to avoid corporate and income taxes,
  - unregistered agricultural businesses which operate outside the tax system.

- Abuse of tax preferences and special regimes
  - misuse of tax exemptions meant for specific industries,
  - artificial restructuring of businesses to benefit from preferential tax regimes.

- Tax base manipulation and underreporting
  - falsifying financial reports to minimise taxable income,
  - using shell companies to create artificial expenses and lower profits.

- Payroll tax evasion
  - paying employees off the books (‘envelope salaries’), reducing payroll taxes.

Comparing these two approaches can provide some insights concerning the similarities and differences related to the context of Ukraine (Table 1.1).

Table 1.1. Tax avoidance schemes comparison

Tax avoidance techniques	Common tax avoidance	Tax avoidance in Ukraine
Income recognition manipulation	Adjusting timing of income recognition to shift taxable income across periods.	Less emphasised. Instead, businesses underreport income through unregistered activities.
Offshore tax havens & profit shifting	Companies establish subsidiaries in tax havens (e.g. Singapore, Mauritius) to shift profits and reduce tax liability.	Strong emphasis on offshore structures, treaty shopping, and round-tripping (repatriating funds disguised as foreign investments).
Transfer pricing abuse	Multinational corporations shift profits by manipulating inter-company pricing.	Similar, but with a focus on transfer pricing audits and BEPS countermeasures.
Debt financing (thin capitalisation)	Companies use excessive debt to deduct interest payments and lower taxable profits.	Not a major concern for Ukraine.
Capital intensity for tax benefits	Businesses with large fixed assets leverage depreciation deductions to reduce taxable income.	Less relevant in the Ukrainian context.
VAT fraud & manipulation	Rarely used in other countries due to legislative differences.	A critical issue, with schemes like carousel fraud, missing trader fraud, and fake VAT refunds costing billions in lost revenue.
Payroll tax evasion (‘envelope salaries’)	Less common issue due to non-standard employment utilisation.	A major issue, with companies underreporting wages to reduce payroll taxes.

Smuggling & customs evasion	Less common due to legislative and digitalisation aspects.	Highly prevalent – includes undervaluing imports, fake transit schemes, and direct smuggling.
Abuse of tax incentives & special regimes	Some companies manipulate tax incentives, but no major emphasis.	Strong emphasis on misuse of tax exemptions, preferential tax regimes, and restructuring to avoid taxation.
Unregistered business activities (shadow economy)	Institutional ownership and governance factors are more common, but informal businesses are less.	A huge problem in Ukraine – cash transactions, unregistered businesses, and fraudulent financial reporting are common.

Source: compiled by the authors based on (Cahyaningrum & Wulandari, 2024; Institute of Social and Economic Transformation, 2024).

1.3. AI and Tax Fraud Possible Solutions: A Case Study of European Countries

Across Europe, tax authorities are leveraging artificial intelligence to improve fraud detection, enhance compliance, and optimise tax collection. AI-powered systems enable real-time risk assessments, automate audits, and analyse vast datasets to identify suspicious transactions, leading to significant financial recoveries. To date, tax agencies have prioritised three key objectives: identifying tax fraud and errors, enhancing the taxpayer experience, and increasing internal operational efficiency (Fig. 1.1).

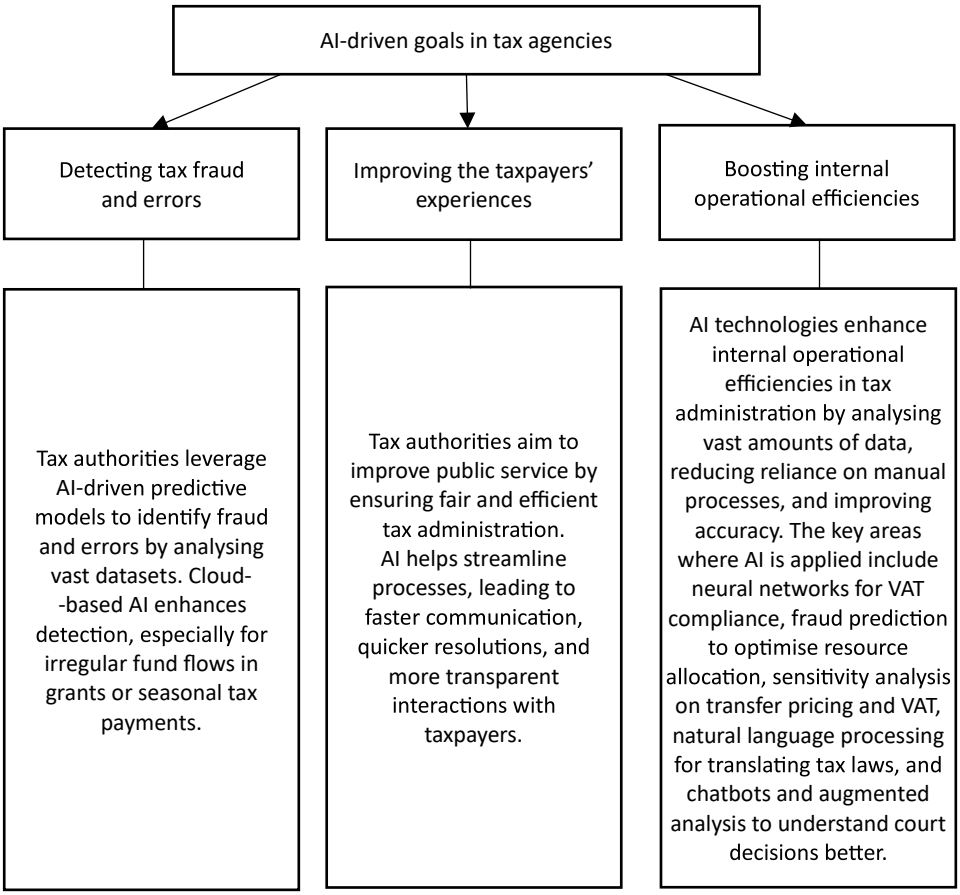


Fig. 1.1. AI-driven goals in tax agencies

Source: compiled by the authors based on (Asquith, 2024b).

One of the primary applications of AI in tax enforcement is identifying discrepancies in financial transactions and tax filings. Italy leads in this area with its VeRa algorithm, which cross-checks tax returns with bank account data to detect inconsistencies. In 2022, this system identified over a million high-risk cases and prevented €6.8 million in tax fraud (PwC, n.d.). Poland employs a similar AI-based approach through its STIR system which analyses daily banking data to detect VAT carousel fraud in near real-time – an improvement over the previous two--month delay. This innovation has contributed to a sharp reduction in Poland's VAT gap, from EUR 6.6 billion in 2017 to EUR 1.7 billion in 2021 (PwC, n.d.). In response to its VAT gap of 17.8% (one of the highest in Europe), Greece followed Austria's example by establishing an AI-driven monitoring centre for real-time VAT fraud detection (Asquith, 2024a).

AI is not only helping tax agencies combat fraud but also improving interactions between tax authorities and taxpayers. Slovakia introduced TAXANA, an AI-powered chatbot, in 2018 to assist taxpayers with queries related to tax returns, electronic filing, and VAT (Financial Administration Slovak Republic, n.d.). Similarly, Latvia's State Revenue Service (SRS) launched the chatbot Toms, which provides automated assistance on general tax matters. These AI tools streamline taxpayer interactions, reducing administrative burdens and making tax compliance more accessible (PwC, n.d.). Additionally, Hungary has experimented with nudging tools, adapting tax communication based on behavioural insights to encourage voluntary compliance (Tamás Czinege, 2019). Other European countries, including Spain, the UK, Ireland, Finland, and Estonia, have also deployed AI-powered virtual assistants to improve tax-related services (SERES, n.d.).

Beyond fraud detection and taxpayer support, AI is enhancing tax agencies' internal processes, making audits more effective and operations more efficient. Austria's Predictive Analytics Competence Centre (PACC) exemplifies this approach, with dedicated AI-driven units focusing on VAT fraud detection, tax audit automation, and customs risk assessment (The Austrian Federal Ministry of Finance, n.d.). In 2023 alone, PACC helped reclaim nearly EUR 185 million in tax revenue and investigated 27.5 million compliance cases (The Austrian Federal Ministry of Finance, 2023). Slovakia and Hungary have also deployed risk-scoring models, which segment taxpayers by risk level, enabling automated selection for audits (Financial Administration Slovak Republic, n.d.; Imrecze, 2016; Tamás Czinege, 2019). These predictive models allow authorities to prioritise high-risk cases while reducing unnecessary investigations.

Looking ahead, Romania is investing EUR 100 million in AI-driven tax solutions as part of its e-Invoice project, aiming to integrate machine learning and robotic process automation to boost VAT revenues by up to 1.0% (Vasilache, 2023). Latvia, meanwhile, has developed an AI--powered taxpayer rating system, using SAP HANA Rule Framework and machine-learning algorithms to assess compliance risk and identify undeclared wages with the accuracy of nearly 90% (PwC, n.d.).

Among the numerous advantages of using AI in tax authorities, it is important to recognise that AI systems are not infallible. Despite their efficiency, errors can occur, and relying entirely on automated processes without proper oversight can lead to significant mistakes. A notable example of this occurred in the Netherlands. In 2013, it was revealed that Bulgarian migrants were exploiting the Dutch social welfare system by registering briefly at an address and retroactively claiming healthcare and housing allowances. The system at the time allowed tax authorities to pay allowances upfront, with eligibility checks conducted afterward, often when the individuals had already left the country (Amaro, 2021). To address such fraud, the Dutch Tax and Customs Administration implemented an AI-powered system to scrutinise family

benefit claims for potential fraud. However, the system began incorrectly flagging legitimate claims as fraudulent. Civil servants in tax authorities, relying heavily on these AI flags, approved the erroneous decisions, leading to thousands of families being wrongly ordered to repay their benefits. This resulted in significant financial hardship for many, with the so-called Dutch childcare benefits scandal (*kinderopvangtoeslagaffaire*) affecting tens of thousands of parents from mostly low-income families (European Parliament, 2022). This case is a stark reminder that AI requires careful supervision to prevent serious consequences.

1.4. AI and Tax Fraud Possible Solutions: The Case of Ukraine

Due to Russian invasion of Ukraine, tax fraud became more dangerous and destructive, as well as a common phenomenon. Revenues from tax and payments are used to finance many governmental spheres of the economy, especially military and social expenditure. Any tax violation reduces the country's ability to maintain its highest priority obligations and can affect the overall economy and market situation.

Different schemes of tax violations led to total budget losses of approximately UAH 354-568 billion (USD 7-11 billion) (Institute of Social and Economic Transformation, 2024). If one compares these losses with overall revenues of the Ukrainian budget in 2023, UAH 3104.8 billion, 11-18% of yearly incomes are missing. These losses are then transformed into an additional burden in terms of expenditures, namely UAH 4441 billion in total and UAH 2098 billion spent on defence. Thus, up to 27% of defence budget was lost due to tax violations (Ministry of Finance of Ukraine, 2024).

AI is not a magic wand and is still limited to keep in line with legislative and compliance requirements, but its efficiency and immunity to human factors are undoubted. AI tools can vary in efficiency due to different use cases, but according to some successful implementations analysed, the average tax fraud detection accuracy is close to 80% (Ariyibi et al., 2024). Implementing such a system in Ukraine can be challenging, but is it worth it?

It is necessary to look closely at the most significant tax gaps found in Ukraine and roughly estimate the possible outcomes. Customs violations and VAT fraud are described in Table 1.2.

Each tax gap can be described from a dual perspective, the human factor and information asymmetry, both of which can be mitigated to a certain extent by implementing some AI tools and features.

Regarding customs undervaluation, both outcomes of AI are valuable. Cross-border data collection and evaluation can significantly reduce the ability to declare unfair customs values, moreover the origin of any product, as well as its price change can be easily tracked. The AI tool will take into account only raw data about products and carriers, no human based biases will occur, and the bribe possibility reduced. The EU TARIC database and Australian Border Force are good examples of such approaches. In general, the existing procedures are aimed to utilise AI capabilities to compare declared import values against historical trade information and current market prices in counterparty countries. Pattern detection is also useful to flag systematic undervaluation as well as fraudulent activities. AI models can mark suspicious shipments for manual or additional inspection based on risk scores or machine learning algorithms (European Commission, n.d.; Outram, 2024).

Table 1.2. Consequences of tax fraud in Ukraine in 2023

Customs violations & smuggling (estimated annual losses: USD 3-5 billion)	
Customs undervaluation	45% of imported goods are undervalued to reduce import duties and VAT.
Interrupted transit & phantom exports	Up to 30% of declared transit goods remain in Ukraine tax-free.
'Ant smuggling' (parcel splitting)	Accounts for 20% of illicit consumer electronics imports.
False classification of goods	15% of customs fraud cases involve tariff misclassification.
Smuggling via Free Economic Zones (FEZs)	Estimated USD 1 billion in goods re-enter the market untaxed.
VAT fraud & manipulation (estimated annual losses: USD 4-6 billion)	
VAT carousel fraud	Causes up to USD 2 billion in tax losses, with missing traders disappearing before VAT is collected.
Fake VAT Refunds via False Export Claims	25% of refund claims in high-risk sectors are fraudulent.
'Invoice mills' & fictitious transactions	Involves 40% of shell companies used for tax evasion.
Construction & services sector fraud	Estimated USD 1.5 billion in lost VAT, primarily in cash-based industries.
Product substitution	Reduces excise tax collections by 10-15% annually, particularly in fuel and alcohol markets.

Source: compiled by the authors based on (Institute of Social and Economic Transformation, 2024).

Interrupted transit & phantom exports utilise similar approaches, while the most efficient way to reduce such a tax gap is to continuously track items. Another method is based on AI's ability to track data integrity via end-to-end tracking of all customs and tax related documents, diminishing possible fraudulent changes, thus the amount of goods declared at any point of the track will remain unchanged until the goods are really delivered to the end customer or have left the territory during transit. If any amount of goods is missing, the system will automatically raise a red flag for the exact operation, carrier, customs broker or any involved party, which can be used for triggering both external tax and customs audit or more detailed AI algorithms. Most of the existing systems use IoT (Internet of Things) devices powered with AI models to track cargo in real-time and flag any route deviations or delays for additional investigation. Blockchain ledgers controlled by AI can be used to ensure data integrity and timely reaction on goods route milestones (European Parliament, n.d.; Singapore Customs, n.d.).

Parcel splitting is not as easy to track and control, hence it is termed as 'ant smuggling'. To mitigate the tax gap created by parcel splitting, AI cannot be used by itself, but can enhance existing systems and predictivity. The main opportunity to avoid 'ant smuggling' is to detect what and how the goods are shipped, especially by individuals or parcels with no cost stated. As already mentioned, AI can only be a supporting tool in this case, enhancing the detection of hidden compartments, excessive repetition of identical parcels, and unusual density patterns as well as part of X-ray scanning software. This can reduce the human factor in the possible detection of unwanted items and flag similar issues. An additional feature – facial recognition – can flag individuals who had been already caught red-handed in cases of illicit imports for additional examination and security checks. Such practices are implemented in e.g. USA and China (U.S. Department of Homeland Security, n.d.; WCO News, 2024).

The false classification of goods is mostly an intentional fraudulent activity to avoid paying the correct amount of taxes and custom duties, but in some cases it can be a simple human error. To reduce this type of tax gap, all invoices and goods should be checked, compared and linked, however in terms of human activities regarding customs this is impossible, and thus AI can give a helping hand. AI powered computer vision can be used for invoices scanning and verification of goods-to-invoice correspondence. Natural language processing AI powered models can provide cross-checking between official customs codes and product description to avoid any sort of misclassification. One more possible solution is to add AI features to automated tax and customs duty verification systems linked to invoices and documents filling systems, thus reducing both intentional and accidental misclassification – the most relevant examples being IBM Watson AI for Customs and India's ICEGATE System (Joubert, 2024; World Customs Organization, 2023).

Smuggling via free economic zones (FEZ) is much easier to detect and reduce, but involves more variables. AI is a big help here, utilising its full power in mapping relations between FEZ, goods, carriers etc., as it can easily identify suspicious patterns in trading across or involving FEZ, as well as detect the misuse of the FEZ status. Another benefit is mapping real and hidden relations between market players to avoid the possibility of fraud, and flag potential subjects for additional inspection (Government of Dubai, 2025; OECD, 2022).

VAT carousel fraud is related to continuous goods routes between a number of parties being the subject of export and import operations more than once. Such operations can be used to reduce VAT payments or even as a way to obtain fraudulent profits. In order to minimise such operations, AI is not only a possible but the necessary solution. AI tools powered with Graph neural networks can analyse the whole flow and route of any kind of goods, marking high-risk traders or trade networks. AI models are also capable of mapping relations between counterparts to identify if any circular transactions exist. Overall, the EU's and Spain's unique systems for VAT flow analysis can be used as examples (Agencia Tributaria, 2024; European Commission, 2019).

Fake VAT refunds via false export claims provide one of the most destructive fraudulent tax schemes in Ukraine. Several approaches already mentioned for tracking goods and monitoring real-time cross-border transit can be used here as well. AI may be used to match customs declarations and statements with real goods movement and VAT refund requests, flagging inconsistency and fraud. Pattern recognition is also useful in terms of industry benchmarks reviewing and predicting possible fraud. The last but not least is IoT involvement to control a goods route and by storing it in blockchain ladder AI tools can verify whether exports actually occurred. The most relevant examples can be found in the UK (HMRC 'Connect') and Korea (eTax) (Daeyong, 2023; Guilherme-Fryer, 2023).

Regarding 'invoice mills' and fictitious transactions, the most relevant solution was also described previously; the natural language processing AI-powered models should be used to verify if invoices and transaction records are consistent. Machine learning can also identify duplicate invoice patterns and flag supply chains that are involved in suspicious activities – the most relevant examples are GST in India and Digital Tax Audit in Germany (Deloitte, 2022; Zetran, n.d.).

Construction & services sector is also suffering from tax fraud, mostly due to cash operations involved. Cash is hard to track and quite difficult to administrate from taxation point of view. AI can help to detect the consequences of some activities that led to creating the tax gap. For example, AI driven tools can analyse bank transaction patterns to identify underreported

incomes or flag companies with excessive VAT credits. An additional AI feature is a reconstruction of financial flows for tax liability base recalculation and comparison (AI Singapore, n.d.; Proximity, n.d.).

Finally, product substitution can be also pointed to. This tax gap generator is mostly related to certain product types that are costly in terms of taxation and easily misclassified due to the existence of lower price products and non-taxable products, for example comestible and industrial alcohol. To reduce the tax gap, AI can also be used. Thus, tax statements are compared to industry-specific production and inventory data to avoid possible misclassification. Computer vision can be used to check barcodes and the appearance of the product itself. Market price tracking is also implemented to flag products declared at unrealistic values – such systems are employed in China and Brazil (General Administration of China Customs, 2024; Johansson Neto et al., 2024).

The implementation of any highlighted approach will be beneficial for both taxpayers and tax authorities. The additional money flow may be to cover budget gaps or as a part of economic development. Moreover, implementation of AI will bring long-term consequences by enhancing all the involved systems and simplifying the observance of tax and custom duties.

While the highlighted method of using AI can mostly be considered as knowledge sharing and best practices, one should also look at some AI tools already implemented in Ukraine. It should be noted that during wartime, most of the existing and planned projects have been suspended, frozen, or forgotten.

The first example of an AI-powered project started in 2019 and was aimed to reduce possible tax fraud related to agriculture. The main idea was to scan and classify agricultural lands in terms of their targeted usage, crop rotation, and exact boundaries of the land parcel. This approach was based on two primary sources, namely satellite and drones' images that were processed with AI tools to create an up-to-date map with additional information layers. Using this information, the tax authorities could track tax flows and possible violations. This was one of the pilot projects, but due to the full-scale invasion it is no longer feasible because the use of drones is prohibited and satellite images are used for defence purposes exclusively (Velykyi, 2019).

One more noted example of AI implemented into the Ukrainian tax administration system is the use by Ukraine's National Agency for the Prevention of Corruption (NAPC) of civil servants' declarations verification. This system is based on an automated verification mechanism and risk assessment for cross-referencing various registry data to identify potential discrepancies. By assessing the declaration's risk rating, the AI system can mark suspicious items for manual verification, reducing burdens and possible manipulations (Kyiv Post, 2023).

Ukraine is capable of leveraging AI and digital technologies to enhance efficiency, transparency, and service delivery within the tax administration, but the current situation and wartime conditions are limiting some possible sources of information and funding for AI implementation. New cases of AI utilisation and implementation of the existing best practices will arise not just to keep pace with, but lead innovation through local and European tax administration systems. This can become a valuable and extensive field for further research.

1.5. Conclusions

By integrating machine learning, blockchain, image recognition, predictive analytics, and natural language processing (NLP), the tax authorities can automate fraud detection, enhance compliance, and significantly reduce tax evasion in both customs and VAT systems. AI-driven solutions enable real-time anomaly detection, automated risk assessments, and cross-border data verification, making them essential tools in modern tax enforcement.

AI-powered network analysis, blockchain verification, and computer vision have already shown success in detecting customs fraud, including undervaluation, smuggling, and the false classification of goods. Similarly, AI applications in VAT fraud detection have proven effective in identifying carousel fraud, fake invoice schemes, and refund manipulations, helping the tax authorities recover billions in lost tax revenue.

Nevertheless, AI alone is not a complete solution. Fraud prevention cannot rely exclusively on automated detection, it requires a holistic strategy that incorporates human expertise. While AI can flag suspicious patterns, tax auditors play a crucial role in reviewing these cases, ensuring that legal principles and taxpayer rights are upheld. A balanced approach ensures that tax enforcement remains accurate, fair, and legally sound.

By combining AI-driven analytics with expert oversight, the tax authorities can build a more transparent, efficient, and data-driven tax system. This synergy helps minimise administrative burden, close tax loopholes, and promote voluntary compliance, ultimately strengthening fiscal governance and securing public revenues.

References

Agencia Tributaria. (2024). *Estrategia de inteligencia artificial*. https://sede.agenciatributaria.gob.es/static_files/Sede/Tema/Agencia_tributaria/Gobierno_abierto/Estrategia_IA.pdf

AI Singapore. (n.d.). *Intelligent Service Quality Monitoring*. https://ai4sme.aisingapore.org/ai-use-case/intelligent-service-quality-monitoring/

Amaro, S. (2021). *Dutch Government Resigns After Childcare Benefits Scandal*. https://www.cnbc.com/2021/01/15/dutch-government-resigns-after-childcare-benefits-scandal-.html

Ariyibi, K. O., Bello, O.F., Ekundayo, T. F., Oladepo, O. I., Wada, I. U. & Makinde, E. O. (2024). Leveraging Artificial Intelligence for Enhanced Tax Fraud Detection in Modern Fiscal Systems. *GSC Advanced Research and Reviews*, *21*(2), 129-137. https://doi.org/10.30574/gscarr.2024.21.2.0415

Asquith, R. (2024a). *AADE Authority Set-up AI-backed Unit to Take on VAT Missing Trader Fraud and Other Tax Evasion*. https://www.vatcalc.com/greece/greece-ai-in-vat-fraud-fight/

Asquith, R. (2024b). *Tax Authorities Adopt AI for Tax Fraud and Efficiencies*. https://www.vatcalc.com/artificial-intelligence/tax-authorities-adopt-ai-for-tax-fraud-and-efficiencies/

Cahyaningrum, A. A., & Wulandari, S. (2024). Determinasi tax avoidance. *Al-Kharaj: Jurnal Ekonomi, Keuangan & Bisnis Syariah*, *6*(5), 3883-3899. https://doi.org/10.47467/alkharaj.v6i5.1370

Daeyong, K. (2023). *Digital Transformation of Tax Administration in the Republic of Korea: Lessons from Experience and Ways Forward*. The Governance Brief, Issue 52. https://doi.org/10.22617/BRF230570

Deloitte. (2022). *Digital Tax Audit*. https://www.deloitte.com/de/de/services/tax/perspectives/digital-tax-audit.html

European Commission. (n.d.). *TARIC*. https://taxation-customs.ec.europa.eu/customs-4/calculation-customs-duties/customs-tariff/eu-customs-tariff-taric_en/

European Commission. (2019). *VAT Fraud: New Tool to Help EU Countries Crack Down on Criminals and Recoup Billions*. https://ec.europa.eu/commission/presscorner/detail/en/ip_19_2468

European Parliament. (n.d.). *Filling the Gap: The EU's Fight Against VAT Fraud*. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2025)767221

European Parliament. (2022). *The Dutch Childcare Benefit Scandal, Institutional Racism and Algorithms*. https://www.europarl.europa.eu/doceo/document/O-9-2022-000028_EN.html

Financial Administration Slovak Republic. (n.d.). *Process Digitalisation*. https://www.financnasprava.sk/en/financial-administration/process-digitalisation

Gaie, C. (2023). *AI, a Weapon Against Tax Fraud*. https://www.polytechnique-insights.com/en/columns/economy/ai-a-weapon-against-tax-fraud/

General Administration of China Customs. (2024). Automating Image Analysis: China Customs Implements New Model for the Development and Deployment of Algorithms. *WCO News*, *104*(2). https://mag.wcoomd.org/magazine/wco-news-104-issue-2-2024/automating-image-analysis-china-customs-implements-new-model-for-the-development-and-deployment-of-algorithms/

Government of Dubai. (2025). *Dubai Customs Launches 'Al Munasiq' Platform Powered by AI to Revolutionize Customs Classification Processes*. https://www.dubaicustoms.gov.ae/en/newscenter/pages/newsdetail.aspx?NewsId=2088

Guilherme-Fryer, G. (2023). *HMRC's AI System Processes Taxpayer Data*. Kreston Reeves. https://www.krestonreeves.com/news/taxpayer-data-now-on-hmrc-ai-system/

Imrecze, F. (2016). Data Analytics as a Tool to Tackle Tax Fraud. In M. Silva Pinto, N. Sawyer, Á. Kővágó (Eds.), *Data-Driven Tax Administration* (pp. 12-17). Intra-European Organisation of Tax Administration. https://www.iota-tax.org/ngsite/content/download/1282/27619

Institute of Social and Economic Transformation. (2024). *Comparative Analysis of the Fiscal Effect of the Use of Tax Evasion/Avoidance Tools in Ukraine*. https://iset-ua.org/en/doslidzhennya/item/219-porivnialnyi-analiz-shem-2024

Johansson Neto, G. P., Farias da Costa, V. C., & Gaspar, W. B. (2024). Brazil's Artificial Intelligence Plan (PBIA) of 2024: Enabler of AI Sovereignty? *The African Journal of Information and Communication*, (34), 1-15. https://doi.org/10.23962/ajic.i34.20424

Joubert, J. (2024). *AI-Driven Decisions with IBM Decisions & Watsonx Orchestrate*. IBM Business Automation Community. https://community.ibm.com/community/user/automation/blogs/jerome-joubert/2024/02/09/ai-driven-decisions-with-ibm-decisions-watsonx-orc

Kyiv Post. (2023). *AI Will Be Used to Check Declarations*. https://www.kyivpost.com/post/25840

Ministry of Finance of Ukraine. (2024). *Budget of Ukraine 2024*. https://mof.gov.ua/en/budget_of_2024-698

OECD. (2022). *Artificial Intelligence and International Trade*. OECD Trade Policy Papers. https://doi.org/10.1787/13212d3e-en

Outram, M. (2024). *How the Australian Border Force Can Exploit AI*. The Strategist. https://www.aspistrategist.org.au/how-the-australian-border-force-can-exploit-ai/

Proximity. (n.d.). *ATO 'Big Data' Strategic Sourcing Project*. https://proximity.com.au/case_studies/ato-big-data-strategic-sourcing-project/

PwC. (n.d.). Role of AI in Transforming How Tax Authorities Work. https://www.pwc.com/lv/en/about/services/IT-services/related-articles/Role-of-AI-in-transforming-how-tax-authorities-work.html

SERES. (n.d.). *How Can Artificial Intelligence Be Used to Help Reduce the VAT Gap?* https://blog.groupseres.com/en/artificial-intelligence-reduce-the-vat-gap

Singapore Customs. (n.d.). *Container Track and Trace*. https://www.customs.gov.sg/businesses/international-connectivity/containertrackandtrace/

Tamás Czinege, C. (2019). *Risk Management in Order to Enhance Compliance of Taxpayers in Hungary*. https://www.iota-tax.org/ngsite/content/download/1423/29493

The Austrian Federal Ministry of Finance. (n.d). *Predictive Analytics Competence Center*. https://www.bmf.gv.at/en/topics/combating-fraud/anti-fraud-units/pacc.html

The Austrian Federal Ministry of Finance. (2023). *Ministry of Finance Generated Around EUR 185 Million in Tax Income from AI in 2023*. https://www.bmf.gv.at/en/press/press-releases/2024--New/August-2024/BMF-generated-around-EUR-185-million-in-tax-income-from-AI-in-2023-.html

U.S. Department of Homeland Security. (n.d.). *United States Customs and Border Protection – AI Use Cases*. https://www.dhs.gov/ai/use-case-inventory/cbp

Vasilache, A. (2023). Statul vrea să folosească Inteligența Artificială pentru colectarea TVA și să facă un Institut de IA de 100 milioane de euro. https://hotnews.ro/statul-vrea-sa-foloseasca-inteligenta-artificiala-pentru-colectarea-tva-si-sa-faca-un-institut-de-ia-de-100-milioane-de-euro-34843

Velykyi, B. (2019). *Shtuchnyi intelekt na sluzhbi Podatkovoi*. DroneUA. Retrieved from https://drone.ua/blogs/news/iskusstvennyiy-intellekt-na-sluzhbe-nalogovoy

WCO News. (2024). *Automating Image Analysis: China Customs Implements New Model for the Development and Deployment of Algorithms*. https://mag.wcoomd.org/magazine/wco-news-104-issue-2-2024/automating-image-analysis-china-customs-implements-new-model-for-the-development-and-deployment-of-algorithms/

World Customs Organization. (2023). *Technology and Innovation in Indian Customs*. https://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/ressources/permanent-technical-committee/239-240/item-ix_technology-and-innovation_india.pdf

Zetran. (n.d.). *AI-Powered GST Compliance and Fraud Prevention*. https://zetran.com/ai-powered-gst-compliance-and-fraud-prevention/

Chapter 2

Diagnostics of Tax Security Threats and Counteraction Mechanisms for Tax Avoidance Schemes

Iryna Chuy

Lviv University of Trade and Economics
ORCID: 0000-0002-8795-4514

Quote as: Chuy, I. (2025). Diagnostics of Tax Security Threats and Counteraction Mechanisms for Tax Avoidance Schemes. In I. Chuy, P. Luty, V. Lakatos (Eds.), *Modern Tools for Fraud Detection: Insights from the V4 and Ukraine* (pp. 20-31). Publishing House of Wroclaw University of Economics and Business.

DOI: 10.15611/2025.40.5.02

2.1. Introduction

Tax security is determined by fiscal sufficiency and tax system efficiency as well as by the predictability of tax relations between the state and taxpayers with the permissible level of tax burden for them. The indicators for assessing the level of tax security include those of the budgetary component of security: the fiscal burden, the level of implementation of planned targets, the cost intensity of administration and effectiveness of tax control, the level of shadow economy, and the tax evasion by individual taxpayers.

The purpose of this chapter was to evaluate both the indicators that affect the tax security, and the ability of society to avoid tax threats and the vulnerability in countering identified threats. To achieve this goal, it was necessary to solve the following tasks: to diagnose the tax security by indicators of fiscal burden, level of gathering, efficiency of administration and effectiveness of tax control measures, and to develop a mechanism to counteract threats and strengthen the tax security of Ukraine as a whole.

Methodology. To build an integrated approach, all the existing and potential factors of threats were analysed. Data from reports of the State Statistics Service of Ukraine, National Bank of Ukraine, Ministry of Finance of Ukraine, OECD and World Bank were used.

The survey was based on an analysis of studies by Ukrainian and international scientists about the essence and nature of tax security over the last 15 years. In addition, to determine the essence and the concept, goals and objectives, methods and principles of the economic nature of the tax security, the main risks, threats, expectations and results of efficient tax security and tax avoidance schemes were identified.

The author applied as the main methods: comparison (factual and planned tax revenues, elements of national tax systems), systematisation and classification (indicators for tax security, indicators classification by stimulants/destimulants), economic analysis (calculation of the security indicator), as well as mathematical and statistical methods (analysis of time series, averages).

The result of an excessive tax burden is the attempt on the part of taxpayers to reduce it. Therefore, in order to strengthen the tax security of the state it is necessary to reduce the scale of tax avoidance by taxpayers and increase the efficiency of tax administration and the effectiveness of tax control.

2.2. Evaluation of Fiscal and Tax Burden of Ukraine and OECD Countries

Tax security indicators of Ukraine for 2016-2022 and their deviation from the threshold values were calculated by the author in Table 2.1. Over the last eight years, the level of fiscal burden (including social security contribution) has increased from 32.8% of GDP in 2016 to 33.4% in 2022, but decreased to 32.4% in 2023. Exceeding the actual value of the indicator above the threshold level existed throughout the analysed period – the highest was in 2018 and 2022 (by 4.1 percentage points).

Table 2.1. Tax security indicators of Ukraine in 2016-2023

Indicators	Threshold level	Years							
		2016	2017	2018	2019	2020	2021	2022	2023
Indicators of fiscal and tax burden									
Fiscal burden (including social security payments), % of GDP	30	32.8	33.8	34.1	33.8	33.9	33.1	33.8	32.4
Labour burden (personal income tax and charge + social security), % of GDP	≤ 13.8[(a)]	11.3	12.3	12.9	13.8	14.0	12.8	16.1	14.9
Total tax burden, % of GDP	≤ 25	27.3	27.8	27.7	26.9	26.9	26.7	25.6	25.1
The level of concentration of tax revenue in the consolidated budget, %	≥ 60	83.1	81.4	83.3	83.0	82.6	87.5	61.2	52.8
The level of concentration of tax revenue in the state budget, %	≥ 60	81.8	79.1	81.2	80.1	79.1	85.4	53.1	53.1
Total coefficient of elasticity of tax revenue	≥ 1	1.41	1.09	0.98	0.73	1.01	0.96	1.96	0.89
Level of shadow economy, % of GDP	≤ 30	33	32	29	28	30	32	n/a	n/a
Indicators of the level of tax collection (fulfilment of planned tasks)									
Total level of tax collection	≥ 1	1.03	1.00	1.00	0.96	1.02	1.04	0.84	0.99
Indicators of administrating efficiency (cost intensity)									
Result ratio (index of expenditures on tax administration, per 100 UAH of tax revenue)	≥ 1	0.96	1.02	1.21	1.09	1.12	1.10	0.96	0.76

Expenditures on tax administrating per permanent population, UAH/person	≤ 258,6[(a)]	147.2	199.4	283.0	280.9	307.3	388.8	n/a	n/a
Expenses for tax administrating per economically active population, UAH/person	≤ 609,4[(a)]	348.4	476.4	664.1	648.7	724.1	925.0	n/a	n/a
Tax debt rate, %	≤ 5	10.7	11	10.3	11.7	9.1	7.3	10.8	8.5
Level of tax integrity, %	≥ 95	95.6	96.8	96.5	95.4	98.4	95.6	98.5	97.2
The efficiency ratio of the fiscal authorities	≥ 5	4.5	3.1	2.9	4.2	1.4	4.0	1.5	3.7

[(a)] Average value for the analysed period.

Source: based on (Chuy et al., 2021).

However, the total tax burden in Ukraine for the analysed period decreased from 27.3 to 25.1%, an increase of the fiscal burden was observed – by direct taxes from 9.1 to 10.9 % of GDP (by 1.8 percentage points). Instead, a decrease by 2.6 percentage points for indirect taxes (from 15 % to 12.4 %) and for taxes on property, resources, capital by 1.4 percentage points (from 3.2 % to 1.8 %) was seen (Fig. 2.1).

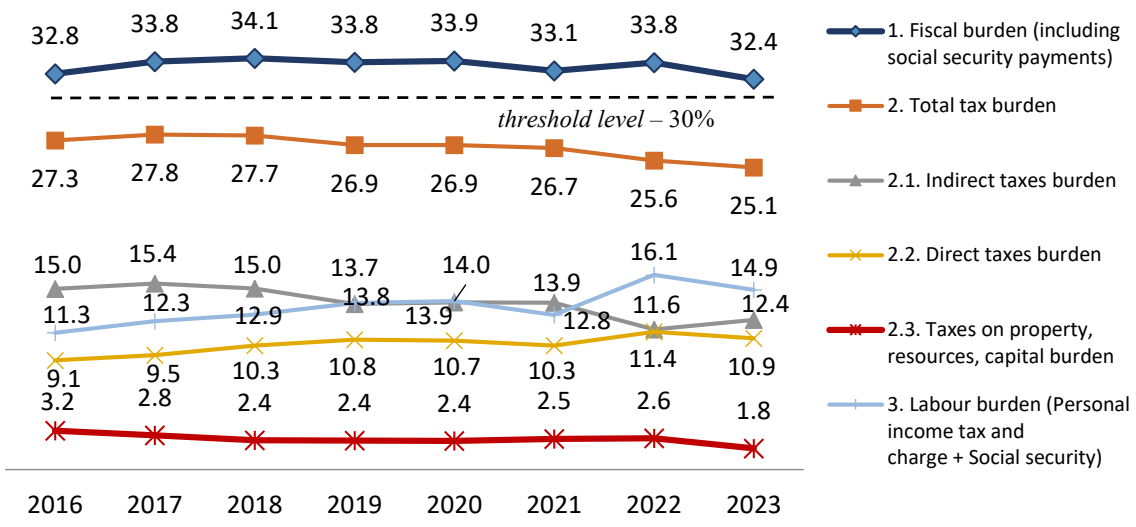
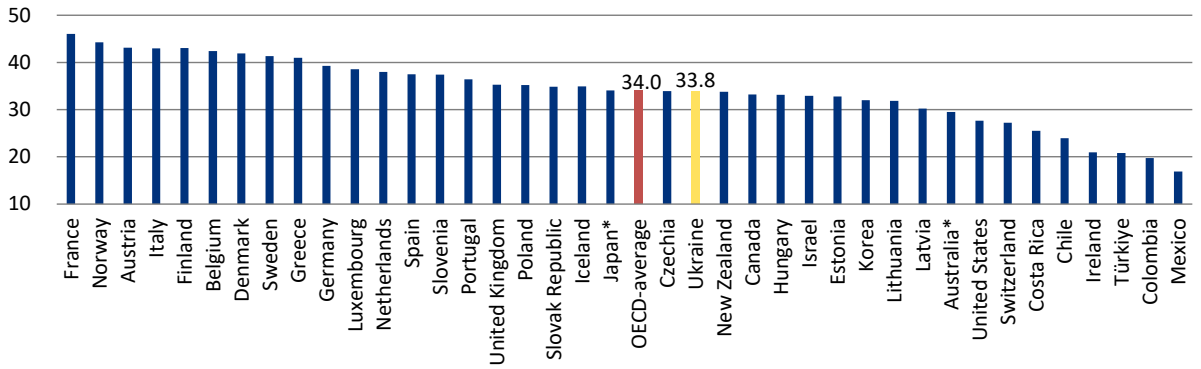


Fig. 2.1. Fiscal and tax burden of Ukraine, 2016-2023, % of GDP

Source: own study.

The tendency to increase the tax burden was demonstrated by the majority of developed countries which are members of the Organization for Economic Cooperation and Development (OECD). The OECD Tax database showed that the average level of tax burden for OECD countries in 2022 was 34% of GDP against 33.6 % in 2016 (Fig. 2.2). Only 15 countries (Austria, Denmark, Sweden, the Netherlands, Spain, Poland, Slovak Republic, Iceland, Estonia, Hungary, Lithuania, Latvia, Switzerland, Ireland, and Türkiye) among the 38 OECD members reduced the level of tax burden during 2016-2022.

The results of econometric analysis by OECD economists showed that economic growth slowdown was due mostly to indirect/consumption taxes, therefore income taxes had a negative impact on tax security, and regular land/real estate taxes were the least harmful



* GDP

Fig. 2.2. Tax burden in OECD countries and Ukraine in 2022, % of GDP

Source: based on (OECD, 2022a).

(Akgun et al., 2017). The problems that reduced the fiscal efficiency of direct taxes and lowered the level of tax security in Ukraine were caused by the low income of the majority of the population, the significant level of tax evasion, and the uneven distribution of the tax burden between the real and financial sectors of the economy (Chuy et al., 2019). The desire to avoid corporate tax was becoming the dominant motive to use offshore schemes (Dubrovsky et al., 2021). Taxes on labour, which include personal income tax, social security payments on both employers and employees and military charges, are harmful because they discourage legal employment and the development of labour-intensive industries, increase the cost of job creation, and instead drive the labour market 'into the shadows' and stimulate labour migration. The state of tax security in terms of labour taxation in Ukraine is exacerbated by low levels of minimum and average wages and their excessive taxation – 11.3% of GDP in 2016 up to 14.9% in 2023. Across OECD countries, the sum of personal income tax (PIT), employer social security contributions (SSCs) and employee SSCs as a share of labour costs for the average worker ranged from 52.6% in Belgium to 0 in Colombia, with an average of 34.6% (OECD, 2022b). The average for labour burden (PIT and SSCs as a percentage of GDP) was 17.8%, with a much higher average applied by Germany (25.4%), Austria (25.1%), Finland (24.8%), Italy (24.7%), and Denmark (24.6%).

The average level of taxes on goods and services in OECD countries in 2021 was 10.8% of GDP and 31.2% of total taxation; these taxes are considered less vulnerable to tax abuse. However, the shadow economy, smuggling, 'grey imports', VAT abuse, excise and import duties, and the sale of counterfeit alcoholic beverages and tobacco products still remain threats to tax security (Dubrovsky et al., 2021).

The least vulnerable to their impact on tax security are taxes on property, since the basis for their accrual is not subject to concealment, and in case of non-payment, there is a pledge in the form of property. The fiscal significance of property taxes averaged 1.8% of GDP or 5.3% of total tax revenue in OECD countries in 2022. In Ukraine, the share of property taxes was much lower; in 2023 it amounted to only 1.8% of GDP and 7% of tax revenue of the Consolidated Budget. The deterioration of the security situation occurred only in cases of fraud in the valuation of property, the use of unlawful benefits or improper administration. The evasion of taxation of extraction of natural resources and underestimation of environmental pollution was possible due to the non-transparency of such activities, concealment of production, monopolisation, and the weakness of state control.

The calculations presented in Table 2.1 showed higher concentration of tax revenue in the state budget – 53.1 %, was higher than in the consolidated budget.

The total coefficient of the tax revenue elasticity was determined via division of the growth rate in tax revenue of the consolidated budget by the growth rate in GDP. The measures of the elasticity coefficient were above 1 in 2016, 2017, 2020, and 2022, which means that tax revenues grew at a higher rate than GDP increased. The ambiguity of trends in the coefficient of tax elasticity is a negative phenomenon caused by an excessive level of tax and fiscal burden, instability of the tax policy of the state and its regulatory influence.

The total level of the tax collection had a negative trend only in 2019. Analysis of the consolidated budget for 2016–2022 showed that in five years out of eight there was an over-fulfilment of the tax revenue plan: in particular, in 2016 – 102.6%, in 2017 – 100.5%, in 2020 – 101.9%, in 2021 – 103.7%, in 2022 – only 84.3% and in 2023 – 99.9%. Due to the strengthening of the hryvnia and the slowdown in import growth in 2020, it was impossible to obtain the planned amount of taxes on imported goods, namely VAT, import duties, and rent payments.

The main fiscal threats were the level of the shadow economy, the culture of taxpayers, the effectiveness of the tax authorities and the stability of the legislation (Golikov, 2016). According to the Ministry of Economy of Ukraine, the level of the shadow economy in 2021 amounted to 32% of GDP, which is 4 percentage points higher than the lowest indicator in 2019. After four years of a positive downward trend, the level of the shadow economy was higher than the threshold level; this requires identifying the causes and finding mechanisms for de-shadowing. During 2018-2020, the level of the shadow economy in Ukraine remained in the safe zone (28-30% of GDP), but its trend was negative. Experts exploring the level of the shadow economy in the field of fuel, alcohol and tobacco production found an extremely high level in these markets (*Assessment of the Level*..., 2024). In 2024, the shadow turnover in the tobacco sector increased to 18% (Q3/2024), and decreased both in alcoholic beverages to 22% and in fuel sectors to 18% (Fig. 2.3). The increase in the level of the shadow economy as a percentage of GDP during 2022-2023 can be explained by the low tax culture, which negatively reflects on the tax security.

The state's losses from the shadow tobacco sector were at least UAH 18-20 billion in 2023, and UAH 7-8 billion in the alcoholic beverages, and UAH 9-10 billion in the fuel sector (*Assessment of the Level*...., 2024).

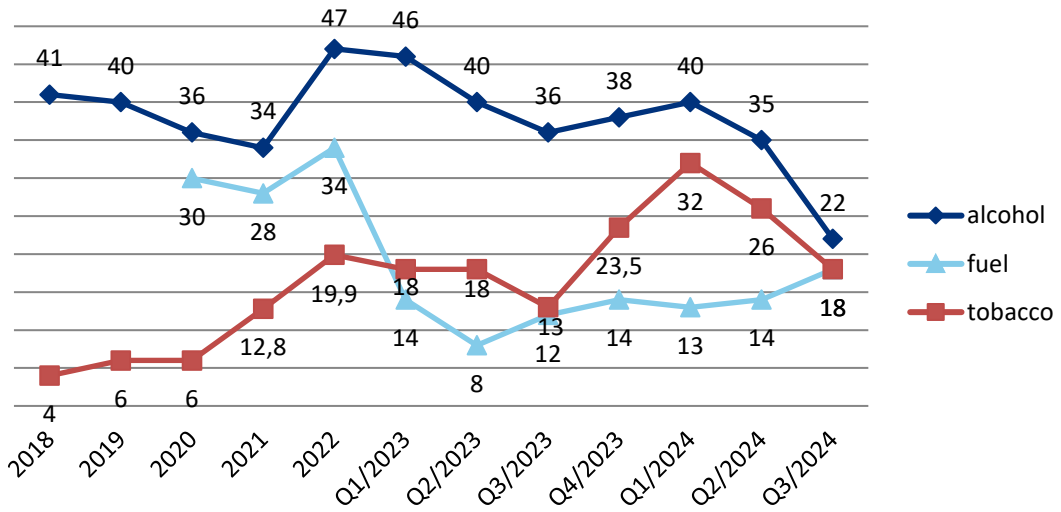


Fig. 2.3. The level of shadow economy turnover in alcohol, tobacco and fuel sectors in Ukraine, %

Source: based on (*Assessment of the Level*...., 2024).

The main reasons were: insufficient awareness of the importance of tax revenue in social and economic development, corruption in tax administrations, inefficient use of funds from the government budget, the examples of impunity for certain individuals or companies for tax violations, abuse of tax benefits, and permanent changes in tax legislation.

2.3. Diagnostics of the Tax Administration Efficiency and Effectiveness of Tax Control

The level of tax security largely depends on the efficiency of the tax authorities. Indicators that measure this include the effectiveness of tax and customs administration and of tax control, especially the cost of the administration process per unit of tax revenue, *per capita* and per economically active population, coefficients of integrity of tax payments and the level of tax debt, as well as the coefficients of efficiency, effectiveness, quality of control measures and payback of fiscal authorities.

Many studies proved the inefficiency of the fiscal authorities, which was confirmed by taxpayers' dissatisfaction with their work, inefficiency of tax administration, excessive control over tax payments and corruption (Chuy et al., 2021; Dubrovsky et al., 2021; Golikov, 2016; Tiutiunyk, 2020). This was also confirmed by the deterioration of Ukraine's Paying Taxes rating, according to which Ukraine's rank was 65 in terms of ease of paying taxes, which is worse than in 2019 by 11 points (World Bank, 2020). The declared automation of processes has not reduced the cost of maintaining the service and combating corruption schemes. The taxpayers spent an average of 328 hours on tax accounting, preparation, reporting and payment in Ukraine, which was higher than in the USA (175 hours), Slovak Republic (192 hours), Germany (218 hours), Czechia (230 hours), and Hungary (277 hours).

The result ratio of administration efficiency calculated by the author (the index of tax administration expenditures per UAH 100 of tax revenue) showed a growing trend in 2016--2018 from UAH 0.96 to UAH 1.21 per UAH 100 of tax revenue, which then decreased to UAH 0.76 in 2023 (Table 2.1). The increase in the cost of fiscal authority's activity had no correlation with the increase in the amount of tax debt and tax evasion. The burden of the cost of tax administration on the economically active population increased over the past eight years, expenditures *per capita* tripled from UAH 348.4 to UAH 925. At the same time, expenditures in the sphere of fiscal, tax and customs policy during 2016-2023 doubled (increased from UAH 6.3 billion to UAH 12.5 billion).

The low efficiency of tax administration was reflected by the increasing tax debt in Fig. 2.4.

The amount of tax debt doubled for the period 2017-2023: from UAH 69.6 billion to UAH 139 billion. The level of written-off 'hopeless' tax debt was determined by dividing its amount by the total amount of tax debt, also showing growing dynamics (from 0.4% at the beginning of 2017 to 14.5% at the beginning of 2021). The amount of written off hopeless debt as of January, 2021 amounted to UAH 15.1 billion (the highest level was 14.5%) – in comparison to 2016, it increased 52 times.

The tax debt rate significantly exceeded the threshold of 5%: in 2016 – 10.7%, 2017 – 11%, 2018 – 10.3%, 2019 – 11.7%, 2020 – 9.1%, 2021 – 7.3%, 2022 – 10.8%, 2023 – 8.5%, which reflected the unsatisfactory state of security. The significant share of tax debt belonged to VAT, corporate tax and rent payments.

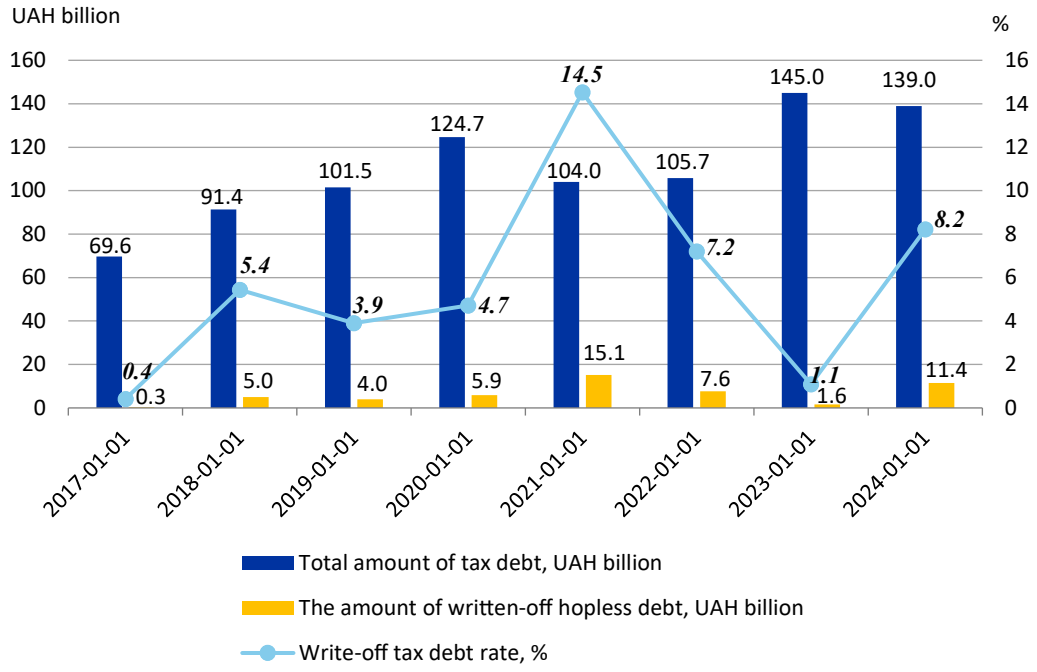


Fig. 2.4. Tax debt and its write-off rate in Ukraine, 2017-2023

Source: based on (State Tax Service of Ukraine, 2024).

The ineffectiveness of the measures taken by the fiscal authorities led to a sharp increase in tax debt during this period, with one of the main measures aimed at paying off tax debt and cancellation of that deemed hopeless.

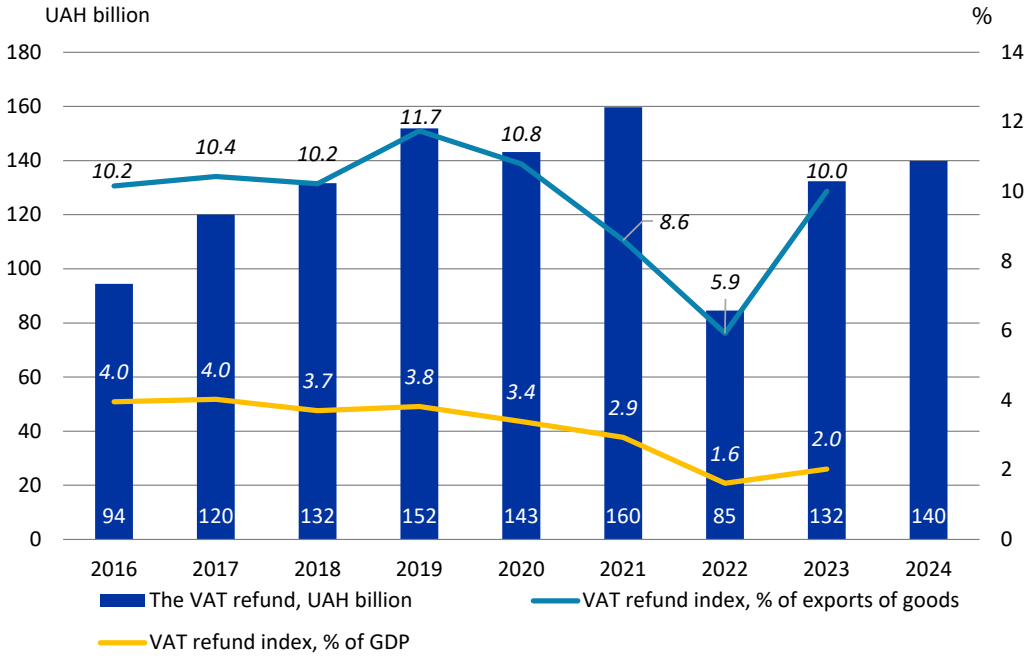


Fig. 2.5. The VAT refunds in Ukraine, 2016-2023

Source: based on (State Tax Service of Ukraine, 2023).

The situation concerning VAT refund is presented in Fig. 2.5. During 2016-2023, the amount of VAT refunds increased from 94 billion UAH to 140 billion UAH. The case of VAT refunds improved

in 2017-2019 as opposed to the background of a slowdown in export growth. The highest value of the VAT refund index was in 2019 (11.7% of exports of goods), but it decreased in 2021 (to 8.6%). After the start of the war in Ukraine in 2022, the government suspended the payment of VAT refunds to exporters in order to save budget funds needed for the military and social needs. In May 2022, the VAT refunding was returned, and in June, the business sector began to receive the first renewed payments again. However, for some entrepreneurs and large enterprises the state tax service has resumed meticulous tax audits.

Currently, in this period of martial law in Ukraine, and because of this, there are changes in the mechanism in VAT refunds: the amount of VAT refunds in 2022 decreased to the lowest value for nine years (UAH 84.6 billion), which is only 5.93% of exports of goods. The VAT amount index as a percentage of GDP decreased from 3.96% to 1.63%. The strengthening of tax control in the direction of desk-audit confirmation of amounts to be refunded and delays in the timing of VAT refunds, have caused distortion of competition and created opportunities for corruption where VAT refunds are carried out manually and only 'selected' entities receive refunds. At the same time, when verifying the correctness of VAT refunds, the tax authorities were faced with the following methods of the illegal overstatement of VAT amounts subject to budget refund, or the overstatement of VAT tax credit as (Ponomaryova & Artyukh, 2022):

- sale of goods at prices that are lower than purchase prices,
- fictitious exports,
- import of goods at reduced prices,
- fictitious tax credit through the creation of fictitious enterprises,
- export of goods that are smuggled back to the customs territory of Ukraine with subsequent registration of their re-export.

Thus, the problem is twofold: the unscrupulousness of taxpayers who are trying to avoid taxation and receive fictitious VAT refunds, and the abuse of the tax authorities in the field of its confirmation.

The effectiveness of tax control is measured by the number of control measures carried out and the amount of additional accrued and collected tax liabilities. After reducing the number of control measures due to the introduction of a moratorium on inspections in 2022, the workload of taxpayers with inspections and reconciliations diminished. Additional charges also decreased: from UAH 28.4 billion in 2016 to UAH 19.6 billion in 2022. The total amount of additional charges for scheduled and unscheduled inspection reports by the State Tax Administration reached UAH 45.9 billion in 2023 (State Tax Service of Ukraine, 2016-2023). However, the average level of tax collection after inspections remained low at 27%, e.g. in 2017 – 31.1%, and in 2023 – 18.7%.

The efficiency ratio of the fiscal authorities reflects the amount additionally accrued to the budgets and public social security funds of Ukraine relative to the amount spent on the maintenance of the controlling authorities. Thus, according to the calculated indicators, ineffective work in the field of risk assessment and tax administrating, poor-quality control, verification work of fiscal authorities, and measures to repay and prevent the accumulation of tax debt and the unreasonableness of additional accrual of taxes were revealed.

2.4. Tax Avoidance Schemes in Ukraine

The most popular in Ukraine were the following tax avoidance schemes: salaries 'in envelopes'; violation of customs rules due to manipulating the customs value of goods and services, interrupted transit, 'grey imports', direct smuggling, illegal VAT refund for exports, fictitious entrepreneurship, in particular 'carousel' schemes, substitution of goods – 'twists' conversion centres, transfer of profits to tax havens and offshores, counterfeiting, schemes of the shadow land rental market, and abuse of tax privileges and special tax regimes.

Analysts declared positive changes in reducing the level of tax evasion in Ukraine in 2022: VAT schemes, offshore schemes, schemes with the land rental, and with the individual entrepreneurs, and salaries 'in envelopes'. However, smuggling, grey imports, counterfeiting, and illegal trade have increased.

The evasion schemes in illegal salaries, grey imports, smuggling, conversion centres, and the understatement of private entrepreneur's income increased in 2023 (Fig. 2.6).

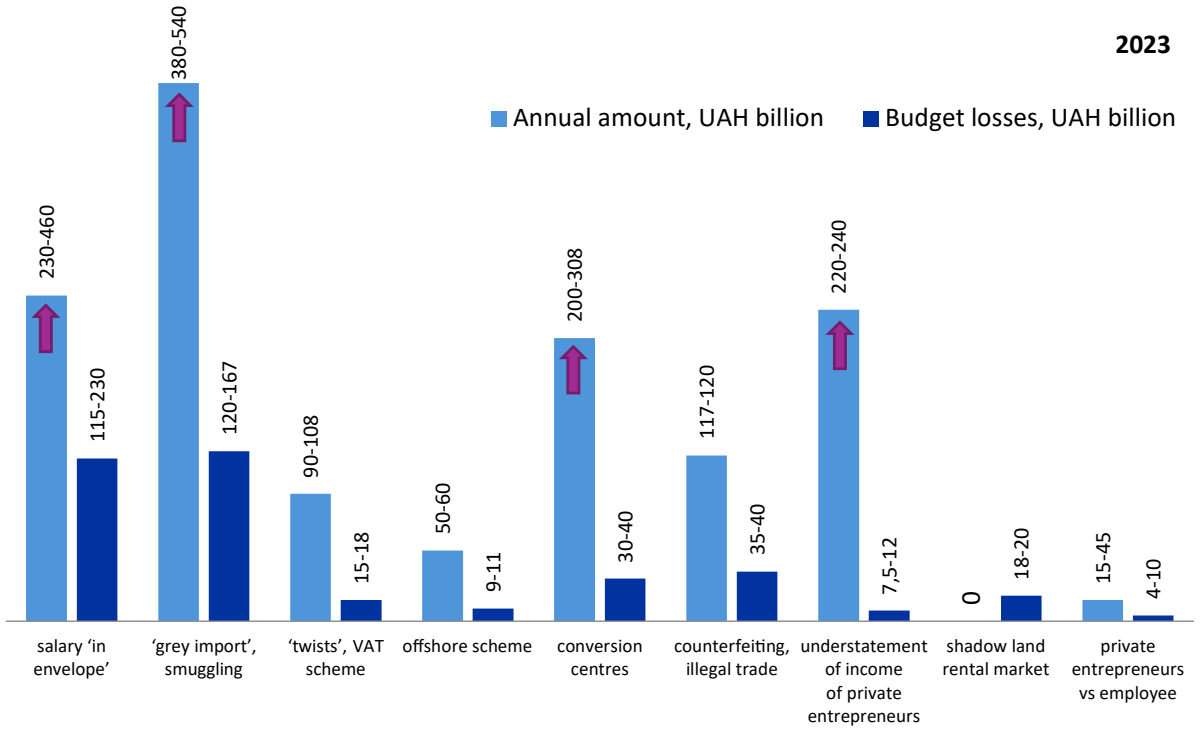


Fig. 2.6. Annual amount and budget losses from tax evasion schemes in Ukraine, 2023

Source: based on (Dubrovsky et al., 2024).

In order to reduce the level of salaries paid 'in envelopes', it is necessary to significantly reduce the labour burden to the target of at least 20% cumulatively (instead of the current 45%), while compensating for lost budget revenue by reducing inefficient expenditures and reforming the collection of resource and property taxes (by increasing its share in GDP).

Budget losses caused by smuggling, mainly due to underestimation of customs value and violations of customs rules, and tightening of customs controls, could improve the situation.

The improvement of administrative efficiency would be possible mainly due to the optimisation of tax payments and the introduction of electronic reporting and taxes payments. The electronic

reports will reduce the administration costs, tighten the communication between tax inspectors and taxpayers, and eliminate the possibility of corruption schemes.

Tax avoidance through offshore schemes, which resulted in a shortfall in tax revenue to the budget, was approximately UAH 9-11 billion annually (Dubrovsky et al., 2024), and provided for the use of legally permitted by instruments, in particular through cross-border aggressive tax planning, tax optimisation, abuse of legal mechanisms or the use of unfair practices (manipulating of residence status in countries with lower tax rates). Unfortunately, the low institutional capacity of controlling bodies to overcome these schemes does not have the effect of reducing corruption risks. The existing anti-offshore instruments in Ukraine (e.g. the transfer pricing control introduced in 2013), have not been properly implemented.

The conversion centres' activities, with the budget losses at UAH 30-40 billion (Fig. 2.6), supplied the informal economy with cash, salaries in envelopes, as well as provided services for manipulation of primary documents and tax invoices.

The problem of excessive tax burden, combined with the weakness of controlling authorities, led to the loss of government control over the market of excisable products, which resulted in the shadow counterfeit market. Counterfeit and illegal trading, in particular excisable goods, generated annually UAH 35-40 billion budget losses in Ukraine. The critical situation with the illegal trade in excisable goods requires the actual launch of the Bureau of Economic Security and the creation of a national system for detecting and tracking excisable goods (alcohol, tobacco products).

Tax evasion through the simplified taxation system can be reduced by: bringing the tax conditions of private entrepreneurs and employees closer; liberalizing the cash register market and simplifying the procedure for their application; reducing the level of excessive fiscalisation of the flat tax payers; simplifying the procedures for registration of employees and liberalising labour legislation.

Using the pseudo private entrepreneurship scheme instead of hiring labour, involved the conclusion of a fictitious contract for the provision of services, according to which non-cash funds were transferred, which, after paying taxes, unified social contributions, remuneration and bank commission, are withdrawn in cash as entrepreneurial income, and returned to the disposal of the company's management. To reduce the amount of such transactions, it is necessary to simplify the process of tax administration and make it much less vulnerable to corruption pressure, in particular by replacing the income tax with the tax on withdrawn capital, simplifying and automating the administration of VAT, reducing the tax burden on wages, eliminating the attractiveness of tax evasion.

2.5. Conclusions

The largest tax abuse schemes in Ukraine in 2023 were grey imports and smuggling, as well as salary in envelopes, and conversion centres. Moreover, the global COVID-19 pandemic became a new threat, along with the introduction of martial law and the destruction of the economic potential of taxpayers due to war losses (this concerns the stability and sufficiency of tax revenue, and the vulnerability of taxpayers to new conditions). The negative impact on the security situation was augmented by the late launch of the Bureau of Economic Security, the low level of investigation of tax crimes, personnel turbulence in the fiscal authorities and often the unprofessionalism of the employees.

Having considered the most typical schemes of avoidance/evasion of taxation in Ukraine, as well as the economic, administrative and legal measures to minimise tax threats, the author proposed the directions for strengthening tax security by reducing the tax burden, increasing the effectiveness of tax control and the efficiency of the tax administration, along with counteracting tax evasion.

The top priority strategic measures are: reducing the tax burden on labour, increasing the fiscal burden on property and resources, reducing the shadow employment, an amnesty for illegally acquired income and property, introduction of public reporting and KPIs on the results of control measures of state fiscal service employees (tax and customs), increasing the level of investigation of tax crimes, raising the level of professionalism and competence of fiscal service employees, motivating taxpayers to reflect real indicators of financial and economic activity in reporting, strengthening the control over the application of tax privileges and deliberate concealment of sales volumes and illegal write-off of expenses, identification and liquidation of intermediary firms in offshore jurisdictions, creation of the database of 'risky' taxpayers and those with a tendency to avoid taxation, and the exchange of information with financial authorities on taxpayers' income.

To strengthen the tax security in Ukraine, it is necessary to reform the tax and customs services, to increase the tax control effectiveness, and to counteract tax evasion. In order to de-shadow the sphere of remuneration and reduce the level of evasion, income taxation in Ukraine needs to be improved in terms of the transition from proportional to progressive taxation of individual income, along with the application of indirect methods for determining the real income of individuals. To improve the tax culture and integrity of taxpayers, it is necessary to activate explanatory and advisory work by employees of the fiscal authorities. De-shadowing and reducing tax evasion constitutes an imperative factor to increase fiscal efficiency.

To improve the efficiency of administration, along with reducing excessive fiscalisation, it is necessary to introduce data monitoring of its cost and effectiveness, together with the simplification of administrative procedures, while strengthening the responsibility of taxpayers for tax evasion. The introduced amnesty for shadow income and illegally acquired assets, along with encouraging investment of funds, should help in reducing tax threats.

References

Akgun, O., Cournède, B., & Fournier, J. (2017) *The Effects of the Tax Mix on Inequality and Growth*. OECD Economics Department Working Paper No. 1447. http://dx.doi.org/10.1787/c57eaa14-en

Assessment of the Level of Shadow by Industry. (2024). Economic Expert Platform [in Ukrainian]. https://economics.org.ua/index.php/nasha-robota/dashbord

Chuy, I., Holdak, S., & Duma, O. (2021). Tax Security as a Factor in Increasing the Fiscal Efficiency of the Tax System of Ukraine. *Bulletin of Lviv University of Trade and Economics*, (65), 151-160 [in Ukrainian]. https://doi.org/10.36477/2522-1205-2021-65-21

Chuy, I., Vlasyuk, N., & Zhurbych, K. (2019). Analysis of Fiscal Potential of Income/Profit Taxes in Ukraine and Foreign Countries. *Entrepreneurship and Trade, 24,* 137-145 [in Ukrainian]. https://doi.org/10.36477/2522-1256-2019-24-21

Dubrovsky, V., Cherkashin, V., & Hetman, O. (2021). *Comparative Analysis of the Fiscal Effect of Tax Evasion/Avoidance Instruments in Ukraine.* Center for Social and Economic Research CASE Ukraine, Institute for Social and Economic Transformation.

Dubrovsky, V., Hetman, O., & Cherkashin, V. (2024). *Comparative Analysis of the Fiscal Effect of the Use of Tax Evasion/Avoidance Tools in Ukraine.* Center for Social and Economic Research CASE Ukraine, Institute for Social and Economic Transformation.

Golikov, S. (2016). Basic Concepts of Tax Security as Part of the Financial Security of Ukraine. *Baltic Journal of Economic Studies*, *2*(1), 25-31.

OECD. (2022a). *Revenue Statistics – OECD Countries*. https://stats.oecd.org/

OECD. (2022b). *OECD Tax Database.* https://www.oecd.org/tax/tax-policy/tax-database/tax-database-update-note.pdf

Ponomaryova, V. & Artyukh, O. (2022) Problem Aspects of VAT Refunds at the Current Stage. *Socio-Economic Problems and the State*, *27*(2), 153-160. http://sepd.tntu.edu.ua/images/stories/pdf/2022/22pvsnse.pdf

State Tax Service of Ukraine. (2016-2023). *Control and Verification Work.* https://tax.gov.ua/diyalnist-/pokazniki-roboti/kontrolno-perevirochna-robota

State Tax Service of Ukraine. (2023). *VAT Refund*. [in Ukrainian]. https://tax.gov.ua/diyalnist-/vidshkoduvannya-pdchv/

State Tax Service of Ukraine. (2024). *Dynamics of Tax Debt.* https://tax.gov.ua/diyalnist-/pokazniki-roboti/dinamika-podatkovogo-borgu/

Tiutiunyk, I. (2020). *De-Shadowing of the National Economy Based on Tax Gap Management* [Doctoral dissertation, Sumy State University]. Sumy, SymSU [in Ukrainian]. https://essuir.sumdu.edu.ua/handle/123456789/77289

World Bank. (2020). *Ease of Doing Business Rankings*. https://archive.doingbusiness.org/en/rankings

Chapter 3

Occupational Fraud in Central and Eastern Europe: Mechanisms, Detection and Prevention Strategies

Bartłomiej Nita

Wroclaw University of Economics and Business
ORCID: 0000-0001-5036-912X

Quote as: Nita, B. (2025). Occupational Fraud in Central and Eastern Europe: Mechanisms, Detection and Prevention Strategies. In I. Chuy, P. Luty, V. Lakatos (Eds.), *Modern Tools for Fraud Detection: Insights from the V4 and Ukraine* (pp. 32-49). Publishing House of Wroclaw University of Economics and Business.

DOI: 10.15611/2025.40.5.03

3.1. Introduction

Occupational fraud is one of the most serious threats to the financial and operational stability of organisations worldwide, affecting private companies, public institutions and non-profit organisations alike, leading to significant financial and reputational losses. According to the Association of Certified Fraud Examiners, organisations lose an average of 5% of their annual revenue due to a variety of employee fraud, translating into billions of dollars in losses annually on a global scale (Association of Certified Fraud Examiners [ACFE], 2024). This fraud can be individual, when committed by a single employee, or organised, when there is collusion between several individuals at different levels of the organisational hierarchy (Shonhadji & Maulidi, 2021).

The importance of the problem of employee fraud is particularly evident in Central and Eastern Europe, including the Visegrad countries (Poland, Czechia, Hungary, Slovakia) and Ukraine. The V4 countries are characterised by rapidly growing economies and often struggle with the challenges of implementing effective internal control systems and anti-fraud mechanisms. Many companies operating in the V4 countries and Ukraine face problems of underfunded internal audit departments, the limited number of risk management professionals and the low level of digitalisation of control processes, all of which causes delays in fraud detection.

Corruption remains a significant challenge for CEE countries, as confirmed by the Corruption Perceptions Index (CPI) 2021-2024 results published by Transparency International. Most countries in the region struggle with systemic problems, such as limited judicial independence, political clientelism and a lack of effective public finance control mechanisms. Despite periodic reforms and anti-corruption initiatives, the CPI results indicate stagnation or regression in the fight against fraud, negatively affecting the transparency of institutions and the level of public trust.

In many countries in the region, high levels of political corruption translate into ineffective anti-fraud measures and weakened law enforcement and oversight bodies. Transparency International draws attention to the links between business and politics that hinder the implementation of effective reforms. At the same time, opaque public procurement procedures and limited support for whistleblowers mean that many cases of corruption go undetected. To effectively reduce corruption in Central and Eastern Europe, it is necessary to strengthen public institutions, increase the independence of the judiciary and develop control and audit mechanisms. Further improvements in this area will depend on political determination, public pressure and cooperation with international organisations promoting transparency and good governance.

The limited financial resources to invest in advanced anti-fraud technologies, such as big data analytics, artificial intelligence systems to detect anomalies or blockchain to secure accounting records, also pose a significant challenge for organisations in the region. While in Western Europe and North America many companies are already using automated transaction monitoring tools, in Central and Eastern European countries fraud detection mechanisms are still mainly based on traditional audits and whistleblowing (Shonhadji & Maulidi, 2021).

The problem of employee fraud in the V4 countries and Ukraine has a significant impact on the region's economies, leading to multi-million dollar financial losses, weakened competitiveness of companies and the erosion of trust in public and private institutions. The growing scale of the phenomenon and the increasing digitalisation of financial processes make it necessary for organisations in the region to adapt their fraud detection strategies to the new challenges. The analysis of fraud perpetration and detection mechanisms in Central and Eastern Europe is an important element in the development of effective risk management and financial prevention strategies.

The aim of this chapter was to analyse the phenomenon of employee fraud in the V4 countries and Ukraine on the basis of available empirical data and reports from the ACFE and Transparency International, which provide systematic information on the scale of the problem, methods of detecting it and the effectiveness of the prevention mechanisms in place. In particular, the chapter attempts to answer the following research questions.

1. What are the most common types of employee fraud?
2. What factors favour the occurrence of fraud in organisations?
3. Which fraud detection methods are most effective?
4. Which anti-fraud controls are most commonly used in the countries analysed and does their effectiveness vary depending on the specific economic characteristics of the country?
5. What are the trends in the detection and reporting of employee fraud in the V4 countries and Ukraine over the past years?

The answers to these questions will provide a better understanding of the scale of the problem and identify potential recommendations for anti-fraud policies in organisations operating in Central and Eastern Europe.

The chapter consists of several sections that systematically analyse the problem of employee fraud. Section 3.2 presents the results of the authors' worldwide research and provides an introduction to the subsequent discussion. Section 3.3 two presents a classification of employee fraud, based on ACFE reports and academic literature. Section 3.4 examines fraud detection methods. Section 3.5 focuses on the diagnosis of labour fraud in the V4 countries and Ukraine based on reports by ACFE and Transparency International. Section 3.6 takes up the issue of

detecting employee fraud in Central and Eastern Europe. The final section summarises the findings of the research and offers recommendations for more effective fraud prevention strategies in Central and Eastern Europe.

The chapter is based on a comprehensive comparative analysis, integrating both academic research and reports on employee fraud, with a particular focus on data for the V4 countries (Poland, Czechia, Hungary, Slovakia) and Ukraine. The research focuses on identifying the types of fraud, their detection mechanisms and the effectiveness of prevention methods, as well as diagnosing the trends and challenges of this phenomenon in Central and Eastern Europe. Several complementary research methods were used to obtain reliable results.

1. A review of the academic literature, providing an in-depth analysis of available academic publications, reports and articles on the mechanisms of employee fraud, its effects and methods of detection and prevention. The analysis covers both the global approach to employee fraud and the specificity of its occurrence in Central and Eastern European countries.
2. The analysis of the reports published by Transparency International and ACFE, which are a key source of empirical information, provides an overview of the data contained in successive editions of *A Report to the Nations*, providing detailed statistics on labour fraud worldwide, including in the CEE region.
3. A comparative analysis aimed at comparing fraud prevention and detection methods used worldwide.

Through a multidimensional research approach, this chapter contributes to a better understanding of the specifics of employee fraud in the V4 countries and Ukraine, the identification of the most common risks, and the identification of the most effective methods of detecting and preventing fraud in organisations operating in the CEE region.

3.2. Occupational Fraud – A Literature Review

Employee fraud is a serious threat to organisations around the world, carried out by employees using their positions to fraudulently obtain financial benefits. Research on this phenomenon focuses on the methods of fraud, its motivations and how to detect it. This review discusses the research contained in a selection of relevant articles, looking at the ways in which fraudsters operate and organisational strategies to reduce fraud losses.

Research on employee fraud has identified several key mechanisms for committing it. Omair and Alturki (2020) pointed to process-based fraud (PBF) which occurs in business processes and involves detailed monitoring of deviations from standard procedures. Such fraud may include false procurement approvals, manipulation of tendering procedures and concealment of unauthorised financial transactions. Omar et al. (2016) conducted a case study of fraud in the automotive industry, revealing that the most common forms of fraud were misappropriation of funds and theft of company resources. They indicated that these frauds were often carried out by mid-level employees who had access to financial resources and warehouses. Additionally, identifying the perpetrators proved difficult due to the limited transaction monitoring mechanisms in the company analysed. Lenz and Graycar (2016) described a spectacular case of embezzlement of AUD 22 million by the CFO of a listed company, which shows that fraud can have different scales and levels of complexity. In this case, the fraud was enabled by a lack of effective board oversight and an over-reliance on a single person with access to key financial

data. A study by Peltier-Rivest and Lanoue (2011) in Canada found that fraud is often perpetrated by managers and those in senior positions, resulting in greater financial losses. These individuals have the ability to manipulate financial statements and make false accounting entries to hide irregularities. It has been indicated that the higher the position in the organisational hierarchy, the greater the opportunity to commit fraud and the greater the difficulty in detecting it. Furthermore, a study in New Zealand (Othman & Ameer, 2022) indicated that small companies are particularly susceptible to fraud because employees often have a wide range of authority and responsibility. Such organisations lack a clear division of responsibilities, allowing individuals to commit fraud without a great risk of detection. Small businesses also often lack developed audit systems, making them more vulnerable to this type of crime.

In addition, the research points to specific types of employee fraud, such as:

- invoice manipulation – falsifying or duplicating invoices to obtain unjustified payments,
- expense reimbursement scams – reporting false or inflated business expenses,
- falsification of financial records – the deliberate distortion of accounting data to conceal embezzlement,
- exploitation of access to computer systems – unauthorised changes to accounting records or modification of payroll systems to obtain additional funds.

The literature review showed that employee fraud is wide-ranging and can take different forms depending on the organisational structure and level of internal control. Understanding these mechanisms is crucial for the effective prevention and detection of fraud in companies and public institutions.

A review of research points to different motivations of perpetrators. Bonny et al. (2015) highlighted factors such as financial hardship and life pressures as the most common reasons for committing fraud. Financial problems, debt and lack of prospects for financial improvement lead many employees to engage in fraudulent activities to avoid economic hardship. The rational choice theory applied to a study of retail price manipulation in Taiwan indicated that perpetrators calculate potential profits and risk of detection before acting (Kuo & Tsang, 2023). Psychological factors such as feelings of unfairness, risk propensity and previous work experience also play an important role in the decision to cheat. In some cases, employees justify their actions by believing that the company does not reward them well enough or treats them unfairly. Maulidi and Ansell (2022) suggested that fraud in the public sector is often linked to corruption and inadequate organisational oversight, making internal control an ineffective tool to counter these practices. Public organisations, particularly those with large bureaucracies, may lack effective anti-fraud mechanisms, which encourages fraud. Research has also shown that motivations for fraud may arise from organisational pressures such as excessive financial performance requirements, an organisational culture that tolerates unethical behaviour and a lack of accountability for financial decisions. In organisations where achieving results 'at all costs' is the norm, employees may feel compelled to manipulate data or falsify records to avoid negative consequences or achieve personal gain.

Various studies indicated the effectiveness of different fraud detection methods. Westhausen (2017) highlighted the growing role of internal audit as a fraud prevention tool. Data shows that organisations with a well-functioning internal audit experience lower fraud losses. An effective internal audit should include systematic operational controls, transaction analysis and investigative auditing in cases of suspected fraud. Research by Shonhadji & Maulidi (2021) stressed the role of whistleblowing and fraud awareness systems in reducing financial statement falsification, however they referred to ethical dilemmas associated with such an

approach, such as fear of reprisals against whistleblowers and potential abuse of the reporting mechanism. Another study in Canada found that the main factors increasing losses from fraud are the position of the perpetrator and collusion between fraudsters, making fraud more difficult to detect. Collaborative fraud is more difficult to uncover as it may involve mutual concealment of irregularities and falsification of evidence (Peltier-Rivest & Lanoue, 2015).

3.3. Types of Employee Fraud

Employee fraud takes many forms and can be classified according to its nature and the mechanisms of the perpetrators. Based on an analysis of the literature (Lenz & Graycar, 2016; Omar et al., 2016; Peltier-Rivest & Lanoue, 2011; Westhausen, 2017), and the ACFE report (2024), employee fraud can be divided into three main categories: asset misappropriation, corruption and accounting fraud.

3.3.1. Misappropriation of Assets

Misappropriation of assets is the most common form of employee fraud, occurring in 89% of the cases analysed in the ACFE report (2024). It refers to activities in which employees unlawfully seize organisation's assets for their own benefit, a problem that affects both small and large companies, as well as the public sector. Losses resulting from the misappropriation of assets can reach hundreds of thousands of dollars per individual case (Peltier-Rivest & Lanoue, 2011).

The main methods of asset misappropriation include:

- Theft of cash and funds – fraudulent expense reimbursements, unauthorised cash withdrawals and company card fraud. In many cases, employees falsify documents to justify non-existent expenses or manipulate payment systems to divert funds into their own bank accounts.
- Theft of stock and goods – common in the retail and manufacturing sectors, where employees use access to company resources to take them illegally. Employees may systematically steal company property, which they then sell on the black market. In some cases, there is collaboration between several individuals, making detection difficult.
- Misuse of business expenses – falsifying invoices, inflating travel costs and reporting non-existent expenses. Submitting forged receipts for hotels, fuel or other business travel costs is common practice. Fraudsters may also bill private expenses as business expenses, thereby obtaining reimbursement.
- Payroll manipulation – employees add fictitious workers or increase their pay through unauthorised changes to the payroll system (Lenz & Graycar, 2016). Fake payrolls may include the introduction of 'ghost workers' who are paid salaries, with the funds going into the accounts of fraudsters. In other cases, alterations involve inflating the salaries of selected employees without the consent of supervisors.
- Use of company resources for personal purposes – the use of company cars, office equipment, raw materials or tools of the organisation for personal purposes, leading to financial losses for the employer (Shonhadji & Maulidi, 2021). In some industries, such as construction or logistics, employees may use company equipment to conduct their own business.

- Appropriation of customer funds – occurs in industries where employees have direct contact with customers and cash payments (Kuo & Tsang, 2023). Employees may manipulate invoices, divert payments or remove evidence of transactions to conceal the embezzlement of funds.

The misappropriation of assets often goes undetected for a long time because employees take measures to hide the fraud, e.g. by falsifying documents or involving colleagues to cover up traces of the crime. Research shows that in most cases the detection of these frauds occurs accidentally or as a result of internal audits and financial analysis (ACFE, 2024). Organisations should implement appropriate controls such as internal auditing, financial data analysis and whistleblowing systems to effectively prevent this type of fraud.

A review of the literature indicates that the misappropriation of assets is one of the most prevalent types of employee fraud, and that the consequences can be serious for both the financial health of the company and its reputation. Putting in place appropriate procedures to monitor and verify transactions is key to limiting losses from this type of activity.

3.3.2. Corruption and Conflicts of Interest

Corruption occurs in 48% of employee fraud cases and includes a variety of illegal activities in which employees abuse their position for personal gain (ACFE, 2024). Corruption can be more difficult to detect than other forms of fraud because it often involves long-term relations between the perpetrators and third parties that are difficult to document. Corruption is particularly prevalent in sectors with high levels of interaction with suppliers and contractors, such as public administration, construction and healthcare (Shonhadji & Maulidi, 2021). The most common forms of corruption are:

- Bribery and extortion – employees accept illegal payments or material benefits in return for favouring certain contractors. This can range from simple bribery to more complex schemes to reward loyal suppliers through preferential treatment.
- Bid rigging – the manipulation of tendering procedures to secure a contract with a particular supplier. In many cases, prior arrangements are made between bidders and decision makers, resulting in a bogus tender process. This type of fraud often leads to higher costs for the organisation and reduced competition in the market.
- Falsification of purchasing decisions – inflating the value of orders in return for benefits from suppliers. This can range from price inflation to the purchase of excessive quantities of goods or services, which are then partially reimbursed to suppliers under unofficial arrangements.
- Conflicts of interest – situations in which an employee makes business decisions that benefit him or her personally, such as hiring relatives for key positions, awarding contracts to companies owned by friends or investing in companies that may benefit from the organisation's decisions. Conflicts of interest can be difficult to detect because they may not formally violate the rules, but lead to decisions that are detrimental to the organisation.

Corruption has far-reaching consequences, not only financially but also in terms of reputation. Organisations that are exposed to corruption often experience a loss of trust from investors, customers and business partners. The ACFE report (2024) shows that companies with anti-corruption mechanisms in place, such as ethical policies, regular audits and whistleblowing systems, have significantly lower fraud losses. It is crucial to educate employees and

implement transaction monitoring systems that can detect unusual patterns of behaviour suggestive of corruption (Westhausen, 2017). It is worth noting that effective anti-corruption requires a multi-level approach, including both preventive measures and investigative mechanisms. The implementation of advanced data analytics and artificial intelligence technologies can help identify suspicious transactions and patterns of behaviour that indicate the possibility of corruption (Kuo & Tsang, 2023). With a comprehensive approach to corruption risk management, organisations can significantly reduce both financial losses and long-term reputational consequences resulting from unethical practices among employees.

3.3.3. Accounting Fraud and Manipulation of Financial Statements

Although accounting fraud is less common, i.e. around 5% of cases (ACFE, 2024), its financial impact is the largest, with a median loss of USD 766,000. These frauds are most often committed by senior management and include:

- Revenue falsification – artificially inflating financial results by recognising non-existent transactions (Kuo & Tsang, 2023). Methods such as 'channel stuffing' – artificially generating orders that are never fulfilled – are often used.
- Hiding costs and liabilities – the manipulation of financial data to present the better financial health of an organisation (Westhausen, 2017). This can include moving operating costs to future periods or hiding liabilities in subsidiaries.
- Misrepresentations in financial reports – falsification of financial statements in order to increase shareholder value or avoid regulatory scrutiny (Lenz & Graycar, 2016). Such actions aim to mislead investors and regulators.
- Overstatement of assets – presenting inflated values of property, inventory or investments to improve a company's balance sheet (Shonhadji & Maulidi, 2021). In some cases, the so-called 'round-tripping' – the creation of fictitious transactions between entities to generate non-existent revenue is used.
- False financial reserves – the creation of excessive or understated financial reserves to manipulate performance in subsequent years (Peltier-Rivest & Lanoue, 2011). This action can lead to the artificial smoothing of an organisation's financial performance.

Accounting fraud can remain undetected for years because the perpetrators are often very knowledgeable about financial mechanisms and audit procedures. Dividing employee fraud into asset misappropriation, corruption and accounting fraud allows for a better understanding of its nature and the implementation of effective counter mechanisms. Academic literature and reports indicate that asset misappropriation is the most common type of fraud, but accounting fraud causes the greatest financial losses (ACFE, 2024).

3.4. Methods of Detecting Occupational Fraud

The effective detection of employee fraud requires a multi-level approach involving both technological tools and organisational oversight mechanisms. Based on the literature (AFCE, 2024; Peltier-Rivest & Lanoue, 2011; Westhausen, 2017), fraud detection methods can be divided into four main categories: internal organisational controls, whistleblowing systems, audits and data analysis, and advanced fraud detection technologies.

3.4.1. Internal Organisational Controls

Internal controls are the primary line of defence against employee fraud. According to the ACFE report (2024), organisations with robust internal control procedures experience significantly lower financial losses related to fraud. Effective controls help to identify irregularities quickly and prevent fraud by reducing the potential for manipulation of an organisation's finances. Key elements of effective control systems include:

- Separation of duties – eliminating situations where one person has full control over financial processes such as payment approval and bookkeeping. In practice, this means that other people should be responsible for approving invoices, some others for posting them and still others for making payments. Introducing such a mechanism significantly reduces the risk of concealing fraud. In addition, companies can introduce rotation procedures for finance-related positions to prevent long-term patterns of fraud.
- Regular financial reviews – the periodic analysis of transactions by independent teams to detect anomalies. Internal audits and periodic reviews help to identify unusual operations that may indicate fraud. Many companies also use unannounced audits to increase the effectiveness of fraud detection. Such audits allow the detection of recurring patterns of activity, such as inflated invoices or suspicious transfers. In addition, it is crucial to audit high-risk transactions and review supplier agreements and contracts to detect potential conflicts of interest.
- Transaction approval procedures – multi-level authorisation of financial transactions to reduce the risk of counterfeiting. This means that each transaction should be approved by more than one person. In particular this applies to transfers above a certain amount, cash withdrawals or agreements with new counterparties. Companies using multi-step controls are less prone to financial fraud. It is also worth implementing IT systems that allow automatic verification of the conformity of accounting documents and financial transactions.
- Monitoring of employee activities – ongoing monitoring of financial operations and transactions by key employees enables the rapid detection of irregularities. Monitoring can range from analysing employees' digital footprints to reviewing access to financial systems. In some cases, analysis of employee behaviour is also used, such as excessive use of access privileges, frequent adjustments to accounting systems or initiating transfers outside standard working hours. On average, companies using tools to monitor employee behaviour report a 25% reduction in fraud losses (ACFE, 2024). Artificial intelligence-based tools can also be used to detect abnormal patterns of financial behaviour, increasing the effectiveness of surveillance systems.
- Limits on transaction amounts and authorisations – putting limits on the maximum amount of transactions that can be authorised by a single employee reduces the risk of large-scale financial fraud. In addition, it is a good idea to limit access to bank accounts and accounting systems to only those who actually need to use them as part of their job duties. Introducing electronic access tracking systems makes it possible to record and analyse users' activities, further safeguarding the organisation against fraud.
- Compliance mechanisms and organisational ethics – the promotion of integrity and an ethical culture within the company has a significant impact on reducing incidents of fraud. Organisations with codes of ethics, mandatory anti-fraud training and regular reminders of the consequences of dishonest actions record significantly fewer incidents of fraud compared to companies without such education (ACFE, 2024). It is worth implementing

ethics programmes that engage employees and build awareness of fraud prevention. Examples include regular workshops for employees on identifying fraud risks and ethical decision-making in a financial context.

Internal organisational controls are most effective when applied comprehensively and in combination with other fraud detection methods. Yet it is worth emphasising that formal procedures alone are not sufficient – regular enforcement and an effective response to detected irregularities are key. Organisations that proactively manage fraud risk through monitoring and audits detect fraud 50% faster on average than those that rely only on responses to whistleblowing reports (ACFE, 2024).

3.4.2. Whistleblowing Systems

According to ACFE (2024), 43% of detected fraud was uncovered through whistleblowing systems. These tools enable employees to report suspicious activities without fear of professional consequences. Effective whistleblowing systems not only increase the likelihood of detecting fraud, but also have a preventative role – potential perpetrators are aware that fraudulent practices may be exposed by colleagues. The most effective whistleblowing systems include:

- Anonymous reporting lines – telephone and online platforms that enable whistleblowing. Employees can safely report fraud without risk of retaliation. Today's whistleblowing systems use encrypted online platforms that guarantee complete anonymity for reporters. Some organisations also bring in third-party whistleblowing answering operators, further increasing employee confidence in the system.
- Whistleblower protection policies – legal and organisational safeguards to prevent reprisals against whistleblowers. Whistleblower protection is a key element of effective whistleblowing systems. The lack of adequate regulations and protection mechanisms can make employees fear the consequences of reporting wrongdoing. Companies implementing whistleblower protection policies ensure that reports are treated confidentially and that whistleblowers will not experience negative professional consequences. In some cases, organisations introduce rewards for whistleblowers to encourage reporting of fraud.
- Training for employees – educational campaigns highlighting the importance of reporting fraud and reporting procedures. Regular training raises awareness of organisational ethics and teaches employees how to recognise and report suspicious activity. Organisations that proactively educate their employees on the importance of whistleblowing, achieve more reports and more effective fraud detection. Training should include both the legal aspects of whistleblower protection and practical case studies to help understand what activities qualify as fraud.
- Multi-channel access to whistleblowing systems – whistleblowing effectiveness increases when organisations offer a variety of ways to report whistleblowing, such as via phone, email, dedicated mobile apps or face-to-face meetings with auditors. A multi-channel approach increases the chances that employees will use the system in the way that is most convenient for them.
- Prompt response to reports – a key element of an effective whistleblowing system is ensuring that each report is investigated and appropriate action taken. Failure to respond to reported wrongdoing can result in a loss of employee confidence in the system.

Organisations should implement protocols for responding to whistleblowing that include conducting an investigation, taking corrective action and keeping whistleblowers informed of the progress of the case.

Despite its effectiveness, there are challenges to implementing whistleblowing systems. One of the main problems is employees' fear of retaliation from superiors or colleagues. In many organisations, the work culture is not conducive to whistleblowing, and individuals who disclose fraud may be perceived as whistleblowers (Lenz & Graycar, 2016). To counter this barrier, organisations should build an ethical culture in which reporting fraud is seen as a responsible corporate action. Another challenge is the risk of abuse of whistleblowing systems by whistleblowers making false accusations. Organisations need to implement vetting procedures to avoid unsubstantiated reports while not discouraging the reporting of actual cases of fraud (Westhausen, 2017). Furthermore, the effectiveness of a whistleblowing system depends on its promotion – employees need to be aware of the existence of such a tool and feel safe using it. Research shows that organisations with well-functioning whistleblowing systems detect fraud on average 46% faster than those that rely solely on audits and data analysis (ACFE, 2024). In addition, organisations with well-developed whistleblowing mechanisms report less fraud-related financial losses, indicating the preventive effect of this fraud detection method.

3.4.3. Audits

Internal audits and data analysis are some of the most effective methods of detecting employee fraud. ACFE research (2024) shows that organisations that regularly conduct financial audits reduce the risk of fraud by more than 50%. Audits not only have a fraud-detection function, but also act as a preventive measure, as awareness of their existence effectively deters potential perpetrators. There are three key approaches to auditing:

- Internal audit – a regular audit of financial records carried out by the organisation's internal department. Internal auditors analyse financial flows and detect anomalies. In addition to traditional methods of analysis, modern internal audits use data analysis software to help identify unusual transaction patterns. Examples include systems that detect repeated payments to the same suppliers or unexplained changes in the accounts (Westhausen, 2017).
- External audit – an independent examination of an organisation's finances conducted by external audit firms. In many cases, external audits reveal anomalies hidden by internal company structures. External auditors have access to comparative industry databases to assess a company's financial performance against market standards, which helps to detect unusual patterns of activity.
- Forensic audit – detailed financial analysis to uncover signs of fraud, often used in criminal investigations, supports legal action and helps to analyse suspicious transactions. A forensic audit includes an in-depth analysis of company correspondence, financial flows and electronic documents to identify collusion between employees and suppliers.

Financial audits, both internal and external, as well as forensic audits, play a key role in detecting and preventing employee fraud, increasing the level of transparency and the effectiveness of organisational controls. Regular financial reviews make it possible to identify irregularities in cash flows, significantly reducing the risk of fraud and increasing employee

accountability for financial decisions. Modern data analysis tools allow auditors to more effectively detect anomalies that may indicate fraudulent activity, and the use of advanced technologies, such as comparative database analysis or monitoring of changes in accounting records, increases the effectiveness of these mechanisms. In particular, forensic auditing which combines financial analysis with forensic investigation, is a valuable tool in cases requiring detailed examination of evidence in the context of larger-scale fraud. As a result, audits serve both a detection and a prevention function, and their effectiveness is a key element of anti--fraud strategies in organisations around the world.

3.4.4. Advanced Fraud Detection Technologies

Advances in technology enable the implementation of modern fraud detection methods, including artificial intelligence and Big Data analytics. The recent report of ACFE (2024) indicated that organisations using analytics tools reduce fraud detection time by 30%, significantly increasing their ability to minimise financial losses. Modern technologies enable the identification of hidden patterns, the real-time detection of anomalies and the automation of audit processes. Key technologies include:

- Big Data analytics – using algorithms to detect anomalies in financial transactions. Big Data analytics makes it possible to process large data sets and identify irregular transaction patterns that may indicate fraud. Examples include the analysis of unusual bank transfers, repeated transactions at short intervals or unexplained transactions in company accounts. In some cases, sophisticated financial network analysis methods are used to detect collusion and fraudulent false invoicing.
- Machine learning – predictive models that identify suspicious patterns of financial behaviour. Machine learning algorithms allow fraud detection by analysing a large number of variables over a short period of time. These models learn from historical fraud data and automatically identify suspicious operations. Systems based on machine learning are particularly effective in detecting invoice manipulation, hidden financial transfers and anomalies in employee spending patterns. Moreover, these tools can also automatically classify fraud risks for individual transactions and signal cases that require further investigation.
- Blockchain – unalterable transaction records that eliminate the possibility of falsifying financial data. Blockchain technology ensures transparency of transactions and eliminates the risk of accounting manipulation. By using a cryptographic record, all transactions are permanent and impossible to change without a trace, significantly increasing the security of financial processes. Blockchain is particularly useful in the financial and commercial sector, where accounting documents are often manipulated and invoices falsified. Companies implementing blockchain in their accounting systems reduce the risk of fraud associated with double invoicing and unauthorised modifications of financial records.
- Natural language analysis (NLP) in fraud detection – modern AI systems use NLP to analyse internal communications within organisations to detect suspicious conversations and information exchanges related to possible fraud. Examples include identifying emails containing wording suggesting collusive bidding and/or financial manipulation.
- Behavioural biometrics and user behaviour analysis – analysing how employees use financial systems allows the identification of unusual activities such as unexpected changes in working patterns, attempts to access confidential data outside working hours or unusual financial operations. Such systems help to detect internal fraud and employee abuse in real time.

The implementation of modern technologies such as Big Data, AI and blockchain significantly increases the effectiveness of fraud detection, enabling the analysis of huge data sets in real time, reducing operational costs and identifying suspicious transactions more accurately. Process automation reduces manual financial reviews and machine learning algorithms minimise false positives. However, their implementation comes with high infrastructure costs, the need for a specialist interpretation of results and the risk of misclassifying transactions. Despite these challenges, organisations that use advanced analytics tools achieve markedly better results in detecting fraud and increasing transparency in financial operations.

3.5. Employee Fraud in the V4 Countries and Ukraine

The reports published by the Association of Certified Fraud Examiners (ACFE) represent the most comprehensive global study of occupational fraud. The first edition of the report was published in 1996 and subsequent versions are released every two years. These documents analyse the methods by which fraud is committed, its impact on organisations, the effectiveness of detection mechanisms and the profile of perpetrators. Each edition of the report is based on data from actual cases investigated by Certified Fraud Examiners (CFEs) and is a key resource for organisations, managers and anti-fraud experts. The reports cover several fundamental areas; the first edition looks at the methods of committing employee fraud, such as the misappropriation of assets, corruption and falsification of financial statements, while another focuses on how fraud is detected, examining the effectiveness of internal audits, transaction monitoring and whistleblowing systems. A profile of fraud-affected organisations is also an important element of the reports, looking at the industries, company size and specifics of the companies most susceptible to fraud.

Another key aspect of the ACFE reports is the characterisation of the perpetrators, covering demographic and occupational analysis, including positions, gender, length of employment and previous incidents of fraud. The reports also provide a detailed analysis of the impact of fraud, assessing the financial impact and the legal consequences for the perpetrators. Each edition culminates in a compilation of best practices for prevention, including recommendations for internal controls, audits, anti-corruption policies and the implementation of technological tools for fraud detection.

Each successive edition of the report provides new data on the evolution of employee fraud. For example, *A Report to the Nations* published in 2018 analysed 2,690 cases from 125 countries, indicating that misappropriation of assets was the most common form of fraud (89% of cases), while falsification of financial statements caused the most losses (ACFE, 2018). The 2020 *Report to the Nations* (ACFE, 2020) noted that organisations were losing an average of 5% of their annual revenue to fraud, with whistleblowing schemes becoming the dominant method of detecting it (43% of cases). The next edition, the 2022 *Report to the Nations*, highlighted the growing role of cryptocurrencies as a tool to hide fraud, indicating that 9% of perpetrators used digital assets to mask fraud (ACFE, 2022). In contrast, the 2024 *Report to the Nations* revealed that the median loss from fraudulent financial statements increased to USD 766,000, with organisations using anti-fraud training and forensic audits reporting significantly lower financial losses (ACFE, 2024). The latest data from 2024 showed that corruption remains the dominant form of fraud in the region, accounting for 71% of all cases. The next most common schemes were invoice forgery (billing fraud – 18%), noncash asset fraud (noncash fraud – 17%), cash theft (cash larceny – 8%) and payroll fraud (11%). The analysis of previous

reports confirmed the trend of the dominance of corruption and fraud related to financial documents. In 2020, corruption accounted for 61% of cases, and falsification of invoices 22%. Furthermore, fraud related to the manipulation of financial statements had a significant impact on an organisation's losses. Compared to other regions, employee fraud in Central and Eastern Europe often also includes skimming, false reimbursements and registering fictitious employees.

The Corruption Perceptions Index (CPI) is a key indicator that assesses the level of corruption in the public sector worldwide. Published annually by Transparency International, it is based on expert analysis and research by international institutions. The CPI scale ranges from 0 to 100, where 0 indicates high levels of corruption and 100 indicates total transparency of public institutions. Corruption remains one of the key challenges for CEE countries, and the Corruption Perceptions Index (CPI) results for 2021-2024 indicate persistent problems with transparency and the rule of law in the region. In Central and Eastern Europe, corruption remains a significant challenge and the CPI results indicate differences in the effectiveness of anti-corruption policies across countries. While some countries are implementing reforms to improve transparency and accountability in public administration, others are stagnating or even regressing in terms of anti-corruption effectiveness. Table 3.1 shows the Corruption Perceptions Index (CPI) for the V4 countries and Ukraine in 2021-2024.

Table 3.1. CPI index for the V4 countries and Ukraine

Year / Country	2021	2022	2023	2024
Poland	56	55	54	53
Czechia	54	56	57	56
Hungary	43	42	42	41
Slovakia	52	53	54	49
Ukraine	32	33	36	35

Source: own compilation based on (Transparency International, 2021, 2022, 2023, 2024).

The analysis of the CPI results in 2021-2024 showed persistent differences in the level of transparency of public administration in CEE countries. Poland maintains a relatively stable CPI, but a slight decline in 2023 indicated problems related to the independence of the judiciary and the weakening of control mechanisms. Czechia stands out for its gradual improvement in the fight against corruption, achieving the highest score in the region in 2023 as a result of strengthening anti-corruption systems and increasing the efficiency of control institutions. Hungary remains one of the most corrupt countries in the European Union according to the CPI, with a persistently low score of 42 in 2022-2024. The main problems include political clientelism, centralisation of power and reduced independence of the judiciary and media. Slovakia also shows little improvement, with a score ranging from 49-52, indicating inadequacies in the enforcement of anti-corruption policies and insufficient transparency of government actions. Ukraine, while still struggling with high levels of corruption, shows the most progress in the CPI, increasing its score from 32 points in 2021 to 36 points in 2023 and 35 points in 2024. This increase is the result of anti-corruption reforms implemented under international pressure, as well as attempts to improve the transparency of public institutions, especially after the Russian invasion in 2022.

The CPI results indicate that the fight against corruption in Central and Eastern Europe remains a major challenge. Czechia and Ukraine show positive trends, while Poland and Slovakia remain stagnant and Hungary experiences a further weakening of anti-corruption mechanisms. The main problems in the region include political clientelism, lack of transparency in public procurement, limited independence of the judiciary and insufficient whistleblower protection mechanisms. In order to effectively curb corruption in the region, it is necessary to strengthen control institutions, increase transparency in public finances and implement more effective tools for prosecuting corruption offences. The future of the fight against corruption in Central and Eastern Europe will depend on the political determination of individual countries and public and international support for transparency and the rule of law.

Transparency International cites among the main causes of corruption various problems in the region:

- weaken the independence of public institutions, including the judiciary and law enforcement agencies, which are often unable to effectively enforce anti-corruption laws,
- high political corruption, manifested in clientelism, non-transparent government spending and restricted access to public information,
- there is the lack of effective protection mechanisms for whistleblowers, with the result that reporting corruption is often associated with reprisals,
- transparency problems in public procurement, where tender procedures are still prone to manipulation and nepotism.

In terms of anti-corruption policies, CEE countries often introduce reforms, but many of them prove to be ineffective due to the lack of consistent implementation and the dominance of political interests. In successive editions of its reports, Transparency International stressed the need to increase the transparency of government activities, strengthen the independence of the judiciary and introduce more effective mechanisms to control the spending of public funds. In conclusion, corruption in Central and Eastern Europe continues to be a significant problem that negatively affects economic development and the quality of governance in the region. In the coming years, the effectiveness of anti-corruption efforts will depend on the determination of the authorities in individual countries and pressure from civil society and international institutions.

3.6. Problems in Detecting Occupational Fraud in Central and Eastern Europe

According to ACFE reports, the most common way to detect fraud in the region is through the whistleblowing system, with as many as 56% of cases detected through whistleblowers' reports. The second most effective method is internal audit (15%), followed by management review (9%) and external audits (6%). The 2022 data showed an increase in the effectiveness of technology in detecting fraud, with transaction monitoring and financial data analysis detecting 36% of cases (ACFE, 2022). However, compared to developed regions such as North America and Western Europe, organisations in Central and Eastern Europe are still less likely to use advanced analytics techniques, which reduces their effectiveness in detecting fraud.

Organisations in Central and Eastern Europe and in Central Asia are implementing a variety of preventive mechanisms. According to ACFE (2024) the most commonly used anti-fraud controls are:

- external audit of the financial statements (94%),
- code of ethics (92%),
- internal audit department (88%),
- reporting lines for whistleblowers (88%),
- management reviews (80%),
- audit committees (79%),
- anti-fraud training for employees (68%),
- analysis of transactional data (56%).

Historical data shows that the level of implementation of control measures is steadily increasing, but the widespread use of predictive analytics and AI systems to identify fraud is lacking. Furthermore, only 8% of organisations have whistleblower reward systems in place, indicating limited employee motivation to report fraud. The analysis of *Reports to the Nations* indicates that CEE countries and Central Asia still face high levels of employee fraud, particularly in the areas of corruption and falsification of financial documents. The predominant method of detecting fraud is whistleblowing, while advanced technologies such as big data analytics and artificial intelligence are used less frequently than in developed countries. Organisations are increasingly implementing effective anti-fraud controls, but the lack of strong incentives for whistleblowers and limited predictive analytics remain challenges in the region.

Between 2018 and 2024, the number of reported cases of employee fraud in Central and Eastern Europe and in Central Asia ranged from 66 to 95 cases per year. Compared to other regions, this represents approximately 4-5% of all the cases analysed globally. Despite the relatively low number of reports, the average loss per case is high, indicating the serious impact of these scams on organisations. Analysing data from 2018-2024, there are some important patterns regarding employee fraud in Poland, Czechia, Hungary, Slovakia and Ukraine. The region is characterised by significant fraud losses and varying fraud detection mechanisms.

Table 3.2 shows the number of reported cases of employee fraud in Poland, Czechia, Hungary, Slovakia and Ukraine, based on the reports published by ACFE. These data allow an assessment of the dynamics of fraud in the region and indicate trends in fraud detection and reporting.

Table 3.2. Number of cases of reported employee fraud

Year	Poland	Czechia	Hungary	Slovakia	Ukraine
2018	12	5	3	2	8
2020	15	7	5	3	10
2022	10	6	4	2	7
2024	8	4	3	1	5

Source: own compilation based on (ACFE, 2018, 2020, 2022, 2024).

The data reveal the number of cases of employee fraud reported in the Visegrad countries (Poland, Czechia, Hungary, Slovakia) and Ukraine in successive editions of *Report to the Nations* published by ACFE. The analysis showed a general downward trend in the number of cases in recent years, which may be due to improved internal control systems and increased awareness of fraud prevention. The analysis of reported cases of professional fraud in the CEE countries demonstrated significant differences between countries in terms of the scale of fraud detected and the effectiveness of control mechanisms. The highest number of cases was reported in Poland and Ukraine, which may be a result of both the larger scale of economic activity in

these countries and more developed fraud detection and reporting systems. In contrast, the number of reported cases was lower in Czechia, Hungary and Slovakia, although there were slight fluctuations in some years. The trend analysis showed a gradual increase in the number of fraud reports in all the studied countries. In Poland the number of cases increased from 12 in 2018 to 21 in 2024, while in Czechia from 7 to 14. The most dynamic increase was seen in Ukraine, where the number of reported cases increased from 14 to 23, which may be due to the more difficult economic situation and insufficient fraud control. The increase in the number of cases in Czechia in 2022 may suggest an improvement in the effectiveness of audit systems and also a greater willingness of companies to report fraud. However, Ukraine stands out with the highest number of professional fraud cases in the region, which may be indicative of systemic corruption problems and insufficiently effective prevention efforts. The lack of adequately developed supervisory mechanisms and economic difficulties encourage the occurrence of fraud and limit the possibilities to combat it effectively. In contrast, in Hungary and Slovakia the number of reported frauds remains relatively stable, which may suggest more effective prevention mechanisms or a lower propensity of companies to report fraud. The relatively low number of reports in Slovakia may be due to the smaller scale of business activity and/or a less developed fraud reporting system.

3.7. Conclusions and Key Findings

Employee fraud is one of the biggest threats to organisations around the world, and its impact goes far beyond the financial dimension to include reputational issues, loss of stakeholder trust and operational destabilisation of companies. This phenomenon is particularly relevant in the context of Central and Eastern Europe, where economic and regulatory specificities significantly affect fraud prevention and detection mechanisms. In the Visegrad countries and Ukraine, challenges related to employee fraud include not only gaps in internal control and audit systems, but also systemic problems such as high levels of corruption or limited resources allocated to modern anti-fraud technologies. The results of the research indicate that despite growing awareness of the problem and the implementation of modern analytical tools, the scale of fraud remains high and its detection largely depends on the effectiveness of reporting mechanisms and the quality of audits carried out.

The analysis of the academic literature and ACFE reports indicated that employee fraud can be divided into three main categories: misappropriation of assets, corruption and manipulation of financial reporting. Asset misappropriation is the most common form of fraud, encompassing activities such as embezzlement of funds, falsification of financial documents, cash theft and payroll manipulation. This type of fraud accounts for around 89% of all reported incidents, making it the dominant problem in both private and public sector organisations. Corruption, although less common than asset misappropriation, in many cases proves more difficult to detect due to structural links between perpetrators and external parties. Its most common forms include bribery, collusive bidding and abuse of purchasing processes. Financial reporting manipulation, although accounting for only around 5% of cases, is the most costly form of fraud, with the median loss associated with this type of fraud being USD 766,000 per case.

Research on fraud detection methods indicates that whistleblowing systems and advanced analytics technologies play a key role in countering fraud. Whistleblowing systems, such as anonymous phone lines or internal reporting platforms, contributed to the detection of 43% of fraud cases between 2020 and 2024. At the same time, developments in technology are

allowing organisations to monitor financial operations more effectively, with the use of tools such as Big Data analytics, artificial intelligence and blockchain enabling the identification of anomalies in real time. However, modern fraud detection methods are only effective if they are properly integrated with traditional controls such as internal and external audits. Regular financial reviews and audits by independent audit teams allow anomalies to be detected at an early stage, minimising potential losses.

The analysis of employee fraud cases in the V4 countries and Ukraine showed significant differences in the effectiveness of prevention mechanisms and the level of fraud reporting. Poland and Czechia stand out for their relatively well-developed internal control systems and legal regulations supporting fraud reporting. Organisations in these countries are increasingly implementing whistleblowing systems and modern fraud detection technologies, resulting in an increasing number of fraud cases detected and the effectiveness of their elimination. Hungary and Slovakia, although gradually modernising their fraud prevention systems, still face limited budgets for anti-fraud activities and fewer specialists for auditing and risk analysis. Ukraine, on the other hand, stands out for its high level of corruption and significant number of fraud cases in the public sector, indicating the need for further regulatory reform and strengthening of institutions responsible for financial supervision.

Despite their broad scope, the analyses presented in this chapter have some limitations that may affect the interpretation of the results. One key challenge is the availability of data, as many cases of fraud go unreported or are only disclosed many years later. Differences in fraud reporting procedures between countries can affect the reliability of comparisons between them, and changing regulations and technological evolution mean that methods that are currently effective may need to be modified in the future. These limitations point to the need for further research to more accurately identify trends in employee fraud and the effectiveness of the prevention methods being implemented.

Future research on employee fraud should focus on several key aspects. Firstly, it will be important to gain an in-depth understanding of the impact of regulation on the effectiveness of fraud detection and to analyse how legislative changes in the V4 countries and Ukraine are reducing the scale of fraud. Secondly, further research should focus on the role of modern technologies, such as artificial intelligence, blockchain or advanced data analytics algorithms, in fraud detection and prevention. It is also worth analysing the psychological and organisational drivers of fraud in order to better understand employee motivations and organisational conditions that may foster or reduce fraud. Another important area of research should be international anti-fraud cooperation, including analysing anti-fraud strategies implemented in Western Europe and comparing them with solutions used in Central and Eastern Europe.

The conclusions of this chapter provide important insights into the specifics of employee fraud in the V4 countries and Ukraine and the effectiveness of their detection mechanisms. Further research in this area can contribute to the development of more effective preventive strategies and the enhancement of internal control systems, which in the long term will reduce financial losses and improve the transparency of organisations in the CEE region.

References

Association of Certified Fraud Examiners [ACFE]. (2018). *Report to the Nations 2018. Global Study on Occupational Fraud and Abuse*. https://www.acfe.com/fraud-resources/report-to-the-nations-archive

Association of Certified Fraud Examiners [ACFE]. (2020). *Report to the Nations 2020. Global Study on Occupational Fraud and Abuse*. https://www.acfe.com/fraud-resources/report-to-the-nations-archive

Association of Certified Fraud Examiners [ACFE]. (2022). *Occupational Fraud 2022: A Report to the Nations*. https://www.acfe.com/fraud-resources/report-to-the-nations-archive

Association of Certified Fraud Examiners [ACFE]. (2024). *Occupational Fraud 2024: A Report to the Nations*. https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2024/2024-report-to-the-nations.pdf

Bonny, P., Goode, S., & Lacey, D. (2015). Revisiting Employee Fraud: Gender, Investigation Outcomes and Offender Motivation. *Journal of Financial Crime*, *22*(4), 447-467. https://doi.org/10.1108/JFC-04-2014-0018

Kuo, C., & Tsang, S. S. (2023). Detection of Price Manipulation Fraud Through Rational Choice Theory: Evidence for the Retail Industry in Taiwan. *Security Journal*, *36*(4), 712-731. https://doi.org/10.1057/s41284-022-00360-3

Lenz, P. J., & Graycar, A. (2016). Stealing From the Boss: Who is Looking? *Journal of Financial Crime*, *23*(3), 613-623. https://doi.org/10.1108/JFC-09-2015-0053

Maulidi, A., & Ansell, J. (2022). Corruption as Distinct Crime: The Need to Reconceptualise Internal Control on Controlling Bureaucratic Occupational Fraud. *Journal of Financial Crime*, *29*(2), 680-700. https://doi.org/10.1108/JFC-04-2021-0100

Omair, B., & Alturki, A. (2020). Multi-Dimensional Fraud Detection Metrics in Business Processes and Their Application. *International Journal of Advanced Computer Science and Applications*, *11*(9). https://doi.org/10.14569/IJACSA.2020.0110968

Omar, M., Nawawi, A., & Salin, A. S. A. P. (2016). The Causes, Impact and Prevention of Employee Fraud: A Case Study of an Automotive Company. *Journal of Financial Crime*, *23*(4), 1012-1027. https://doi.org/10.1108/JFC-04-2015-0020

Othman, R., & Ameer, R. (2022). In Employees We Trust: Employee Fraud in Small Businesses. *Journal of Management Control*, *33*(2), 189-213. https://doi.org/10.1007/s00187-022-00335-w

Peltier-Rivest, D., & Lanoue, N. (2011). Thieves From Within: Occupational Fraud in Canada. *Journal of Financial Crime*, *19*(1), 54-64. https://doi.org/10.1108/13590791211190722

Shonhadji, N., & Maulidi, A. (2021). The Roles of Whistleblowing System and Fraud Awareness as Financial Statement Fraud Deterrent. *International Journal of Ethics and Systems*, *37*(3), 370-389. https://doi.org/10.1108/IJOES-09-2020-0140

Transparency International. (2021). *Corruption Perceptions Index 2021*. www.transparency.org/cpi

Transparency International. (2022). *Corruption Perceptions Index 2022*. www.transparency.org/cpi

Transparency International. (2023). *Corruption Perceptions Index 2023*. www.transparency.org/cpi

Transparency International. (2024). *Corruption Perceptions Index 2024*. www.transparency.org

Westhausen, H. U. (2017). The Escalating Relevance of Internal Auditing as Anti-Fraud Control. *Journal of Financial Crime*, *24*(2), 322-328. https://doi.org/10.1108/JFC-06-2016-0041

Chapter 4

Challenges and Reforms in the Accounting System of Ukraine: The Impact of War and Transition to International Standards

Hana Bohušová

Ambis University
ORCID: 0000-0002-3669-4230

Quote as: Bohušová, H. (2025). Challenges and Reforms in the Accounting System of Ukraine: The Impact of War and Transition to International Standards. In I. Chuy, P. Luty, V. Lakatos (Eds.), *Modern Tools for Fraud Detection: Insights from the V4 and Ukraine* (pp. 50-61). Publishing House of Wroclaw University of Economics and Business.

DOI: 10.15611/2025.40.5.04

4.1. Introduction

Ukraine's accounting system has evolved considerably since gaining independence in 1991. Before this, Ukraine was part of the Soviet Union's centrally planned economy, where accounting practices were focused on meeting state-controlled targets rather than serving as tools for decision-making in a market economy. This legacy has complicated Ukraine's efforts to adopt International Financial Reporting Standards (IFRS), which prioritise transparency and comparability – both critical for attracting foreign investment and integrating into global markets (Ernst & Young [EY Ukraine], 2023).

In 2012 the transition to IFRS became mandatory for large enterprises as part of Ukraine's broader economic reforms aimed at fostering transparency, improving financial disclosure, and attracting foreign investment. However, the shift has been far from uniform. Small and medium-sized enterprises (SMEs), in particular, continue to rely on National Accounting Standards (NAS), which retain many characteristics of the outdated Soviet-era system. The difficulties in fully implementing IFRS have been exacerbated by the ongoing war, which has caused economic instability, disrupted supply chains, and further complicated regulatory enforcement (Organisation for Economic Co-operation and Development [OECD], 2023; International Monetary Fund [IMF], 2023).

This paper examines the evolution of Ukraine's accounting system, focusing on the challenges posed by the transition to IFRS amidst the war and the lingering influence of Soviet-era practices. It also explores the broader issues of corruption, the informal economy, and bureaucratic inefficiencies that obstruct Ukraine's ability to maintain transparent and reliable financial reporting.

4.2. Aim and Methodology

The main aim of this paper is to provide a comprehensive analysis of the current state of accounting regulations in Ukraine, with a specific focus on the challenges posed by the ongoing conflict and the transition from Soviet-era practices to modern international standards. The objectives are as follows:

- to evaluate the progress of IFRS implementation and identify the barriers hindering its full adoption,
- to assess the impact of the war on accounting practices and financial reporting,
- to analyse the role of corruption, bureaucratic inefficiency, and the informal economy in complicating regulatory compliance,
- to propose recommendations for improving Ukraine's accounting system and aligning it more closely with international standards.

The research methodology used in this paper is based on qualitative analysis, utilising secondary sources such as international financial reports, government documents, scientific articles, and industry reports (OECD, IMF, EY, PwC). These sources provide insights into Ukraine's regulatory framework, the challenges associated with IFRS adoption, and the economic and political factors influencing financial reporting. The analysis includes:

1) a historical review of Ukraine's accounting transition from Soviet practices to IFRS,
2) a comparative analysis of the regulatory frameworks governing NAS and IFRS,
3) an evaluation of the war's direct and indirect impacts on business operations and financial reporting practices,
4) a review of the informal economy and its influence on transparency and financial stability.

4.3. Results and Discussion

4.3.1. Historical and Theoretical Background: Soviet Legacy and Reforms

The legacy of Soviet accounting continues to influence Ukraine's financial reporting system. Soviet-era accounting was designed for a centrally planned economy, with a primary focus on detailed bookkeeping and reporting to meet state quotas. This system did not prioritise transparency, flexibility, or the provision of investor-oriented information, which are the core principles of IFRS. After Ukraine gained independence in 1991, the country initiated reforms aimed at modernising its accounting practices and aligning them with international standards (Solodchenko & Sucher, 2005).

In the past two decades, Ukraine has made substantial efforts to transition its accounting system toward International Financial Reporting Standards (IFRS) to facilitate integration into the global economy. The adoption of IFRS aims to enhance transparency, comparability, and reliability in financial statements – key factors in attracting foreign investment and building trust in Ukraine's financial markets (PricewaterhouseCoopers [PwC Ukraine], 2023). One of the most significant reforms occurred in 2012, when IFRS became mandatory for large enterprises and publicly traded companies. This change was intended to improve the reliability of financial statements, enhance comparability, and foster greater investor confidence.

However, SMEs which comprise a significant portion of Ukraine's economy, were allowed to continue using National Accounting Standards (NAS), which are aligned with but not identical to IFRS. These standards aim to provide a simplified framework for smaller businesses while maintaining some level of international comparability (Deloitte Ukraine, 2023a).

The foundation of Ukraine's national accounting system is the Law on Accounting and Financial Reporting in Ukraine. Initially enacted in 1999 and amended multiple times, this law requires large enterprises and public interest entities to apply both NAS and IFRS which serve as the legal foundation for accounting practices. NAS were developed to standardise accounting practices across various sectors and ensure transparency, consistency, and comparability in financial statements.

Regulatory bodies such as the Ministry of Finance, the National Bank of Ukraine, and the State Fiscal Service play a pivotal role in overseeing and implementing accounting reforms. These institutions are tasked with developing and enforcing accounting standards, providing guidance, and ensuring compliance (Verkhovna Rada of Ukraine, 2024). Additionally, international organisations like the International Monetary Fund (IMF) and the World Bank have played instrumental roles in promoting accounting reforms. Despite these efforts, the adoption of high-quality accounting standards has often faced resistance due to deeply entrenched local practices and vested interests.

The conceptual framework is essential in modernising Ukrainian NAS. It provides a set of underlying principles, assumptions, and guidelines that form the foundation for developing accounting standards, preparing financial statements, and ensuring consistency in financial reporting. This framework offers a structured approach to understanding the objectives and elements of financial reporting, helping standard-setters, auditors, and accountants apply accounting principles consistently across various entities and industries. It also aims to improve the quality and transparency of financial information, ensuring that financial statements provide relevant, reliable, and comparable data to investors, creditors, regulators, and management.

While Ukrainian NAS is primarily based on the Soviet-era principles – focusing on tax compliance and regulatory reporting – the conceptual framework has increasingly evolved to align with IFRS. This gradual alignment reflects Ukraine's ongoing efforts to modernise its financial reporting system and improve transparency.

Unlike IFRS or US GAAP, the conceptual framework (CF) in Ukrainian NAS is not codified in a single, standalone document. Instead, its principles are embedded within various legislative and regulatory documents such as the Law on Accounting and Financial Reporting in Ukraine, government regulations, and specific accounting standards issued by the Ministry of Finance of Ukraine.

The NAS conceptual framework defines the principles and objectives of financial reporting, ensuring that financial statements provide useful information for decision-making. It emphasises the importance of relevance, reliability, comparability, and understandability in financial reporting. NAS financial statements include a balance sheet (Statement of Financial Position), an income statement (Statement of Comprehensive Income), a cash flow statement, a statement of changes in equity, and notes to the financial statements. The guidelines also cover the recognition and measurement of assets, liabilities, income, and expenses.

As of the latest update, there are 30 individual NAS standards in Ukraine, each addressing specific aspects of financial reporting and accounting practices.

The Ministry of Finance of Ukraine is responsible for issuing, updating, and enforcing NAS. These standards are periodically reviewed and updated to ensure alignment with IFRS and to address new accounting challenges and practices. Regulatory bodies such as the State Fiscal Service ensure compliance with NAS through regular audits and inspections. However, compliance issues, economic instability, and a significant informal sector present challenges to the effective implementation of NAS. This detailed overview of the structure of NAS in Ukraine underscores the comprehensive nature of the standards, which are designed to align with international practices and promote transparency and reliability in financial reporting.

The most recent list of active NAS is presented below.

NAS 1: General Requirements for Financial Reporting.
NAS 2: Consolidated Financial Reporting.
NAS 6: Correction of Errors and Changes in Financial Statements.
NAS 7: Fixed Assets.
NAS 8: Intangible Assets.
NAS 9: Inventory.
NAS 10: Accounts Receivable.
NAS 11: Liabilities.
NAS 12: Financial Investments.
NAS 13: Financial Instruments.
NAS 14: Leases.
NAS 15: Revenue.
NAS 16: Expenses.
NAS 17: Income Tax.
NAS 18: Construction Contracts.
NAS 19: Business Combinations.
NAS 21: Effects of Changes in Foreign Exchange Rates.
NAS 22: Effects of Inflation.
NAS 23: Disclosure of Information on Related Parties.
NAS 24: Earnings per Share.
NAS 25: Simplified Financial Reporting.
NAS 26: Employee Benefits.
NAS 27: Non-current Assets Held for Sale and Discontinued Operations.
NAS 28: Impairment of Assets.
NAS 29: Segment Reporting.
NAS 30: Biological Assets.
NAS 31: Finance Costs.
NAS 32: Investment Property.
NAS 33: Exploration and Evaluation of Mineral Resources.
NAS 34: Share-Based Payments.

The coexistence of two parallel accounting frameworks – NAS and IFRS – has resulted in confusion and inconsistencies in financial reporting, especially for businesses that operate in both domestic and international markets (PwC Ukraine, 2023).

4.3.2. Regulatory Challenges: IFRS vs. NAS

The dual use of IFRS and NAS within Ukraine's regulatory framework poses significant challenges for businesses. While large enterprises are mandated to comply with IFRS, smaller companies continue to follow NAS, which retains elements more closely aligned with Soviet-era accounting practices.

This coexistence has led to inconsistencies in financial reporting, complicating the efforts of investors and regulators to assess the financial health and performance of companies across different sectors (EY Ukraine, 2023). Tables 4.1 and 4.2 compare the most significant standards between the two frameworks.

Table 4.1. Comparison of Ukrainian NAS and IAS/IFRS

Ukrainian NAS	IAS/IFRS equivalent	Key differences	Alignment level
	Conceptual Framework	IFRS: Principles-based, emphasising the economic substance of transactions over their legal form. IFRS is geared towards providing useful information to a wide range of stakeholders, including investors. NAS: Rules-based, heavily influenced by Soviet-era practices. The focus is primarily on compliance with tax and regulatory frameworks, rather than investor-oriented financial reporting.	Low
NAS 1: General Provisions for Financial Reporting	IAS 1: Presentation of Financial Statements	NAS 1 follows the structure of IAS 1 but lacks some disclosure requirements that IAS 1 mandates such as a statement of comprehensive income.	Partial
NAS 2: Consolidated Financial Statements	IFRS 10: Consolidated Financial Statements	IFRS 10 requires consolidation based on control, not just ownership. NAS 2 focuses more on legal ownership.	Partial
NAS 7: Fixed Assets	IAS 16: Property, Plant, and Equipment	NAS 10 is similar to IAS 16 but uses historical cost more frequently. Revaluation under NAS is less common and less detailed.	Partial
NAS 8: Intangible Assets	IAS 38: Intangible Assets	NAS 12 follows IAS 38 but lacks some of the detailed guidance on the recognition and amortisation of intangible assets.	Partial
NAS 9: Inventories	IAS 2: Inventories	NAS 11 aligns with IAS 2 on the measurement of inventories at the lower of cost or net realisable value. However, IAS 2 has more detailed requirements on write-downs.	High
NAS 11: Liabilities	IAS 37 – Provisions, Contingent Liabilities, and Contingent Assets	NAS 11 is generally less detailed but aligned with the same principles.	Partial
NAS 12, 13: Financial Instruments	IFRS 9: Financial Instruments	IFRS 9 requires financial instruments to be measured at fair value, while NAS 25 generally uses historical cost.	Low

NAS 14: Leases	IFRS 16: Leases	NAS 14 still allows off-balance sheet treatment for operating leases, while IFRS 16 requires recognition of leases on the balance sheet (right-of-use asset and liability).	Low
NAS 15: Revenue NAS 18: Construction Contracts	IFRS 15: Revenue from Contracts with Customers	IFRS 15 is more detailed and principles--based, using a 5-step model for revenue recognition. NAS 23 is simpler and tends to recognise revenue earlier.	Low
NAS 21: Effects of Changes in Foreign Exchange Rates	IAS 21: The Effects of Changes in Foreign Exchange Rates	NAS 21 aligns with IAS 21 in accounting for foreign currency transactions, but IAS 21 provides more guidance on translation differences in financial statements.	High

Source: own elaboration.

Table 4.2. Impact on financial statements

Aspect	IFRS Impact	NAS Impact	Impact on Financial Statements
Revenue Recognition	Delayed revenue recognition. ↓	Early recognition. ↑	Lower short-term profits under IFRS. NAS may overstate profits due to earlier recognition.
Inventory Valuation	Lower of cost or NRV. ↓	Historical cost ↑	IFRS shows more conservative asset valuations. NAS may inflate total assets.
PPE Revaluation	Fair value revaluation. ↑	Historical cost. ↓	IFRS increases asset values through revaluation. NAS understates assets, especially in inflationary environments.
Leases	Right-of-use asset and liability recognized. ↑	Off-balance sheet. ↓	IFRS results in higher liabilities and assets. NAS hides long-term obligations from the balance sheet.
Financial Instruments	Fair value introduces volatility. ↓	Historical cost reduces volatility. ↑	IFRS introduces volatility in asset and liability values, impacting profit/loss. NAS offers stable but potentially outdated valuations.
Impairment of Assets	More frequent and earlier impairments. ↓	Delayed recognition. ↑	IFRS lowers asset values through regular impairment tests. NAS delays impairment, leading to overstated asset values.

Source: own elaboration.

Empirical studies demonstrated that the adoption of IFRS had significant financial impacts on Ukrainian companies, particularly in sectors with large physical assets and financial instruments. Skrypnyk and Ambarchian (2015) found that companies applying IFRS reported lower short--term profits due to deferred revenue recognition and earlier recognition of impairments. However, the revaluation of property, plant, and equipment under IFRS often resulted in higher total assets, providing a more accurate reflection of market conditions compared to NAS, which relies on historical cost.

Empirical Findings Summary

- Revenue Recognition: companies under IFRS recognized 15% less revenue in the initial period compared to NAS.

- PPE Valuation: the revaluation of assets under IFRS led to a 12% increase in total assets in asset-heavy industries.
- Lease Liabilities: IFRS capitalises leases, resulting in a 20% increase in liabilities compared to NAS, which keeps leases off the balance sheet.

Regulatory differences pose a significant barrier to the full adoption of IFRS in Ukraine, primarily due to inconsistencies between local laws and international standards. Research highlights several factors contributing to this issue. Many countries, including Ukraine, have only partially adopted IFRS as they must align their local regulations with international standards. According to Nobes and Zeff (2016), countries converging their local standards with IFRS often face delays in regulatory approval or find themselves adjusting IFRS to fit their local context, which can dilute the effectiveness of full adoption.

Gray (1988), and Finch (2009) discussed how national accounting systems, deeply rooted in legal and tax frameworks, can conflict with IFRS adoption. In Ukraine, NAS is heavily influenced by the tax system, making it difficult to fully shift to IFRS principles, which focus more on investor transparency. This gap between tax-driven accounting and investor-driven IFRS is a common barrier in transitioning economies (Ball, 2006; Mirza & Holt, 2011; Zeghal & Mhedhbi, 2006).

Furthermore, IFRS's complexity and the evolving nature of Ukraine's financial markets pose challenges, particularly for small and medium-sized enterprises (SMEs), in adopting these standards. According to C. N. Albu and N. Albu (2012), the local economic environment is not yet fully aligned with the sophistication required for IFRS. The lack of widespread IFRS expertise and advanced accounting systems also presents a significant barrier. There is a shortage of qualified accounting professionals in Ukraine, particularly those with IFRS expertise. This gap hinders businesses' capacity to implement international standards effectively. Many accountants in Ukraine were trained under Soviet-era practices and may not have received the necessary education or professional development to implement modern international standards effectively. This lack of expertise leads to discrepancies in financial reporting. Panasyuk et al. (2021) identified several barriers to the full adoption of IFRS by Ukrainian companies, including legislative gaps, the complexity of IFRS, lack of expertise, high costs, and resistance to change. Legislative gaps arise from inconsistencies between Ukrainian legislation and IFRS requirements. Compared to national GAAPs, IFRS is perceived as more complex and difficult to apply. Transitioning to IFRS entails significant costs, such as system upgrades and staff training, which pose a considerable challenge for Ukrainian businesses.

Note that Ukraine's accounting system, influenced by Soviet-era practices that prioritise tax compliance over financial transparency, further complicates the adoption of IFRS. The dual requirement to maintain separate systems for tax accounting and financial reporting under IFRS adds another layer of complexity. These challenges, particularly the costs associated with training professionals and implementing advanced systems, remain substantial barriers to IFRS adoption in Ukraine.

4.3.3. Impact of the War on Accounting Practices

The Russia-Ukraine war, which began on February 24, 2022, has had far-reaching consequences for businesses globally and within Ukraine.

Impact on companies operating in Ukraine

The war has had profound global economic implications, disrupting supply chains, causing fluctuations in commodity prices, and increasing inflationary pressures. These challenges have significantly impacted companies operating in or connected to Ukraine, Russia, and neighbouring countries, as highlighted by Deloitte (2023a). Businesses have been forced to carefully evaluate the financial effects on their assets, liabilities, and overall operations.

For companies with operations in Ukraine, the war has created numerous financial reporting challenges. Key considerations include the impairment of long-term assets, disruptions to supply chains, and the recognition of losses resulting from closures and damages in affected areas. Additionally, foreign currency volatility and the increased risk of cyberattacks add to the complexities faced by these businesses. The heightened uncertainty has necessitated a thorough evaluation of direct and indirect exposures, which must be reflected in financial statements.

In the USA, the SEC has issued guidance on financial disclosures related to the war, emphasising areas such as risk factors, management discussion and analysis (MD&A), and internal control over financial reporting. These directives aim to ensure transparency and provide stakeholders with a clear understanding of the war's financial impact on affected companies.

Impact on Ukrainian companies

The war in Ukraine has profoundly disrupted accounting practices, creating a cascade of economic instability, interrupted supply chains, and inflationary pressures that challenge the ability of businesses to maintain accurate and transparent financial records (OECD, 2023). These disruptions have led to production delays, logistical challenges, and inventory management issues, complicating revenue recognition and resulting in frequent discrepancies between financial forecasts and actual outcomes (World Bank Group, 2023).

PwC (2022) stated that approximately 60% of companies operating in Ukraine reported the need to assess impairment indicators due to physical damage, loss of control over assets in occupied territories, or a significant drop in expected cash flows. More than 40% of surveyed businesses faced material interruptions to supply chains, directly impacting inventory levels and valuation. Furthermore, over 30% of firms noted delays in the recognition of revenue due to contract cancellations or fulfilment difficulties, with long-term projects requiring reassessment under IFRS 15. PwC emphasised the need for Ukrainian companies to provide detailed disclosure of risk exposure, asset revaluation impacts, and liquidity concerns in line with IAS 1 and IAS 10, as war-related events often qualify as either adjusting or non-adjusting events depending on timing and severity.

Inflation has compounded these difficulties, particularly in the valuation of assets and the measurement of liabilities. In response to these challenges, some businesses have turned to creative accounting methods to present more favourable financial outcomes, undermining the accuracy of financial reporting and complicating stakeholders' decision-making processes (Deloitte Ukraine, 2023a). According to PwC (2022), currency fluctuations and the hryvnia devaluation led to exchange losses averaging 15–20% on foreign-denominated liabilities.

Regulatory enforcement has also been weakened due to the ongoing conflict. Key oversight institutions, including the Ministry of Finance and the National Bank of Ukraine, have struggled

to maintain effective regulatory compliance amid the war's disruptions (IMF, 2023). Consequently the government has shifted its priorities from long-term financial reforms to ensuring immediate economic survival.

4.3.4. Barriers to Transparency and Compliance

Despite Ukraine making efforts to modernise its accounting system, several obstacles continue to impede progress toward achieving transparency and alignment with international standards. Corruption remains a significant challenge, undermining the effective enforcement of accounting regulations. Transparency International (2023) ranked Ukraine 104th out of 180 countries in its 2023 Corruption Perceptions Index, with a corruption score of 36. Corruption undermines the enforcement of financial reporting standards by leading to inconsistent penalties for non-compliance, thereby reducing regulatory accountability and weakening overall transparency.

Recent study by Noy and Dabamona (2024) confirmed that the Russia-Ukraine conflict has caused persistent disruptions in accounting regulation and practice across Ukraine. The conflict has amplified regulatory divergence and significantly weakened enforcement mechanisms – particularly in the eastern and southern regions – where access to company records and audit functions has been curtailed. According to the World Bank Group (2023) assessment, over 45% of Ukrainian businesses reported disruption in their ability to maintain regular financial records due to displacements, damaged infrastructure, or loss of personnel. Furthermore, 30% of companies faced delays in the preparation or audit of their financial statements (World Bank Group, 2023). In response to these challenges, firms increasingly adopted conservative reporting approaches, including earlier impairment recognition, expanded risk disclosures, and precautionary valuations of property, plant, and equipment. Deloitte Ukraine (2023b) noted that nearly two-thirds of Ukrainian firms revised their 2022 disclosures to reflect war-related risks and supply chain uncertainties. Technological innovations are also gaining traction: around 18% of large Ukrainian enterprises reported piloting blockchain-based or automated reporting solutions to enhance data reliability and reduce manual reporting errors (PwC, 2023). These empirical trends underline the urgent need for Ukraine to implement adaptive regulatory reforms, support institutional resilience, and enhance international collaboration to safeguard transparency, comparability, and market trust amidst ongoing geopolitical uncertainty.

A large sector of the economy operates informally, with minimal or no financial reporting, which complicates efforts by the regulatory bodies to ensure accurate and transparent disclosures (Golovko et al., 2022). According to World Economics (2024), the size of Ukraine's informal economy is estimated to be 44.2%, representing approximately USD 388 billion at GDP PPP levels. As a result, substantial financial activity remains unaccounted for in official financial statements, enabling companies to evade taxes and bypass regulatory oversight. Additionally, corruption undermines the consistent application of financial reporting standards, as penalties for non-compliance are often applied arbitrarily, further eroding accountability.

Another significant obstacle is Ukraine's dual regulatory framework, which mandates the use of International Financial Reporting Standards (IFRS) for large enterprises and publicly traded companies, while smaller and medium-sized enterprises (SMEs) adhere to National Accounting Standards (NAS). This dual system leads to inconsistencies in financial reporting across the

economy, making it challenging for investors to compare financial statements across sectors and companies. Moreover, it complicates regulatory oversight, as enforcement agencies must ensure compliance with two distinct sets of standards. This division stretches resources and reduces the effectiveness of consistent enforcement.

Deloitte (2022) identified economic instability as a further factor complicating financial reporting in Ukraine. Inflation, currency fluctuations, and disruptions to supply chains have created an unpredictable business environment, making it difficult for companies to maintain accurate and reliable financial records.

The transparency of public companies in Ukraine, particularly in terms of audited financial and non-financial reporting, was critically low, as noted by Makarenko and Serpeninova (2017). However, since then Ukraine has made significant progress in aligning its regulatory framework with international standards according to the Generis Global Legal Services report (2024). This progress has provided greater clarity regarding compliance obligations for businesses and contributed to a fairer business environment. Annual financial statements, which companies in Ukraine are required to prepare, serve as a key tool for ensuring transparency. The accuracy of these statements is verified through external audits, which safeguard their integrity, yet the failure to meet these requirements can lead to severe consequences, including financial penalties, reduced investor confidence, and operational restrictions.

Based on the aforementioned analysis, several recommendations can be made to address the challenges in Ukraine's financial reporting system:

Recommendations

1. Reinforce regulatory oversight: the Ukrainian government should allocate increased financial and human resources to its key regulatory bodies, such as the Ministry of Finance and the National Bank of Ukraine, to enable more robust enforcement of IFRS compliance and financial transparency standards (World Bank Group, 2023).
2. Modernise and digitise reporting infrastructure: modernising and digitising the reporting infrastructure in Ukraine is a crucial step towards improving efficiency, transparency, and resilience. Ukraine should accelerate the adoption of secure digital platforms e.g. XBRL and AI-supported audit tools to improve the timeliness, reliability, and accessibility of financial reports and make compliance with international standards more efficient (PwC, 2023). This transition should be supported by government initiatives.
3. Develop crisis-responsive reporting guidelines: Ukraine's regulators should publish crisis--specific accounting guidance to standardise the reporting of asset impairments, supply chain disruptions, and operational losses. This would help align practices and mitigate inconsistencies during future conflict or emergency periods (Deloitte Ukraine, 2023).
4. Enhance international cooperation and technical assistance: collaboration with international organisations such as the World Bank, IFRS Foundation, and the EU can support regulatory capacity building and offer technical expertise to improve Ukraine's resilience to future shocks (Noy & Dabamona, 2024).
5. Expand IFRS training and certification: given the shortage of qualified IFRS professionals, universities and professional associations in Ukraine should expand certification programmes and practical workshops targeting war-affected regions and SMEs (EY Ukraine, 2023).

These recommendations collectively aim to strengthen Ukraine's financial reporting framework, align it with global standards, and promote a more robust and transparent business environment.

4.5. Conclusions

Ukraine's accounting system is at a critical crossroads. While significant strides have been made in aligning with IFRS, the country's progress has been hindered by the ongoing war, economic instability, and the enduring influence of Soviet-era practices. The coexistence of IFRS and NAS continues to create challenges for businesses and regulators, making it difficult to maintain consistent financial reporting across sectors.

Despite these challenges there is a clear path forward. Strengthening regulatory frameworks, investing in professional education, and addressing corruption are essential steps in modernising Ukraine's accounting system. By fostering greater transparency and improving compliance with international standards, Ukraine can attract more foreign investment and continue its integration into the global financial system.

References

Albu, C. N., & Albu, N. (2012). International Financial Reporting Standards in an Emerging Economy: Lessons from Romania. *Australian Accounting Review, 22*(4), 341-352. https://doi.org/10.1111/j.1835-2561.2012.00196.x

Ball, R. (2006). International Financial Reporting Standards (IFRS): Pros and Cons for Investors. *Accounting and Business Research, 36*(sup1), 5-27. https://doi.org/10.1080/00014788.2006.9730040

Deloitte (2022). *Accounting and Reporting Implications Resulting from the Ukraine War*. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/audit/us-audit-accounting-and-reporting-implications-resulting-from-the-ukraine-war.pdf

Deloitte Ukraine. (2023a). *Supply Chain Implications of the Russia-Ukraine Conflict*. https://www2.deloitte.com/us/en/insights/industry/public-sector/ukraine-reconstruction-plan.html

Deloitte Ukraine. (2023b). *Accounting and Reporting Implications Resulting from the Ukraine war*. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/audit/us-audit-accounting-and-reporting-implications-resulting-from-the-ukraine-war.pdf

Ernst & Young [EY Ukraine]. (2023). *How IFRS Reporting Is Impacted by Global Volatility and Vulnerability*. https://www.ey.com/en_ua/insights/ifrs/how-ifrs-reporting-is-impacted-by-global-volatility-and-vulnerability

Finch, N. (2009). Towards an understanding of cultural influence on the international practice of accounting. *Journal of International Business and Cultural Studies*, *2*(1), 1-6.

Golovko, M., Kotina, H., & Dolbneva, D. (2022). Accounting Information System of Ukrainian Business: Evolution, Challenges, and Perspectives. *Accounting, Auditing & Accountability Journal, 35*(5), 1297-1317.

Generis Global Legal Services (2024). *Understanding Compliance and Reporting Requirements for Companies Operating in Ukraine*. https://generisonline.com/understanding-compliance-and-reporting-requirements-for-companies-operating-in-ukraine/

Gray, S. J. (1988). Towards a Theory of Cultural Influence on the Development of Accounting Systems Internationally. *Abacus, 24*(1), 9-12.

International Monetary Fund [IMF]. (2023). *Ukraine. Selected Issues Papers*. IMF Country Reports 23/400. https://www.elibrary.imf.org/downloadpdf/view/journals/002/2023/400/002.2023.issue-400-en.pdf

Makarenko, I., & Serpeninova, Y. (2017). Public Companies' Transparency in Ukraine: Key Regulatory Requirements. *Public and Municipal Finance, 6*(1), 8-14. https://doi.org/10.21511/pmf.06(1).2017.01

Mirza, A. A., & Holt, G. J. (2011). *IFRS: A Quick Reference Guide.* John Wiley & Sons.

Nobes, C. & Zeff, S. (2016). Have Canada, Japan, and Switzerland Adopted IFRS? *Australian Accounting Review, 26*, 284-290. https://doi.org/10.1111/auar.12131

Noy, I., & Dabamona, J. (2024). War and Financial Statements: Assessing the Impact of the Russia-Ukraine Conflict on International Accounting and Reporting Standards. *Advances in Applied Accounting Research, 2*(2), 71-82. https://doi.org/10.60079/aaar.v2i2.177

Organisation for Economic Co-operation and Development [OECD]. (2023). *Ukraine Economic Snapshot*. https://www.oecd.org/en/topics/sub-issues/economic-surveys/ukraine-economic-snapshot.html

Panasyuk, V., Ovsiuk, N., Volchek, R., Azarenkov, G., Volenshchuk, N., & Tyvonchuk, O. (2021). The Process of Forming Accounting Policies of Ukrainian Enterprises by International Financial Reporting Standards. *Universal Journal of Accounting and Finance, 9*(5), 1199-1211. https://doi.org/10.13189/ujaf.2021.090529

PricewaterhouseCoopers [PwC]. (2022). *Accounting Implications of the Russian Government's Invasion of Ukraine*. PwC In Depth. https://viewpoint.pwc.com/dt/us/en/pwc/in_depths/2022/2022/2201_acctimplrussinvasukr.html

PwC. (2023). *Implications of the Russian Government's Invasion of Ukraine*. In depth No. US 2022-01. https://viewpoint.pwc.com/dt/us/en/pwc/in_depths/assets/indepth20221updated0505.pdf

Skrypnyk, M. I., & Ambarchian, V. C. (2015). Comparison of Ukrainian GAAP with IFRS and US GAAP: Are There More Differences or Similarities? *Проблеми теорії та методології бухгалтерського обліку, контролю і аналізу, 33*(3), 353-364.

Solodchenko, M. & Sucher, P. (2005). The Development of Accounting in Ukraine. *Journal of Accounting in Emerging Economies, 3*(1), 65-86.

World Bank Group. (2023). *Ukraine Rapid Damage and Needs Assessment – February 2023*. https://documents.worldbank.org

Transparency International. (2023). *Corruption Perception Index 2023*. https://images.transparencycdn.org/images/CPI-2023-Report.pdf

Verkhovna Rada of Ukraine. (2024). Law on Specifics of State Supervision (Control) in the Sphere of Economic Activity Regarding Natural Persons – Entrepreneurs and Legal Entities Using the Simplified System of Taxation, Accounting, and Reporting. https://zakon.rada.gov.ua/laws/main

World Economics. (2024). *Ukraine's Informal Economy Size*. https://www.worldeconomics.com/National-Statistics/Informal-Economy/Ukraine.aspx

Zeghal, D., & Mhedhbi, K. (2006). An Analysis of the Factors Affecting the Adoption of International Accounting Standards by Developing Countries. *The International Journal of Accounting, 41*(4), 373-386. https://doi.org/10.1016/j.intacc.2006.09.009

Chapter 5

Creative Accounting: Deceptive Practices and Strategies for Prevention

Jan Pěta

Brno University of Technology
ORCID: 0000-0001-6309-3601

Quote as: Pěta, J. (2025). Creative Accounting: Deceptive Practices and Strategies for Prevention. In I. Chuy, P. Luty, V. Lakatos (Eds.), *Modern Tools for Fraud Detection: Insights from the V4 and Ukraine* (pp. 62-75). Publishing House of Wroclaw University of Economics and Business.

DOI: 10.15611/2025.40.5.05

5.1. Introduction

When external entities seek to assess the financial position of a company, they most often rely on financial statements issued in Central Europe. These statements provide a comprehensive overview of a company's financial performance – not only at a specific point in time but also in terms of its development over time. Key financial documents include the balance sheet, income statement, and cash flow statement, which together allow an assessment of a company's stability, profitability, and liquidity.

Investors use financial statement data to analyse a company's past performance and try to predict its future performance. This process plays a crucial role not only in investment decisions, but also in the assessment of a company's creditworthiness by banks and other creditors. Financial statements therefore have a wide range of applications, from assessing a company's financial health to determining its market value – an essential factor in cases such as company sales or initial public offerings.

Company owners and management responsible for preparing financial statements are aware of the significant impact these reports can have on how their company is perceived by external stakeholders. As a result, some may adopt strategies that involve accounting adjustments to present their company in a more favourable light than reality suggests. Such practices may include artificially inflating revenues, understating expenses, or misvaluing assets and liabilities, which can create a misleading picture of a company's financial stability.

Recent decades have seen several accounting scandals with far-reaching consequences not only for the companies involved but also for the financial system as a whole. Among the most notorious were the collapses of Enron and WorldCom, which resulted in billions of dollars of losses and severely undermined investor confidence in the transparency of financial reporting.

In Europe, the best-known case was that of the Italian company Parmalat. These incidents led to the introduction of stricter regulations, such as Directive 2006/43/EC on statutory audits, which imposes stricter requirements on firms authorised to audit financial statements.

In some cases accounting fraud has been seen as a contributing factor to wider economic crises, including the global financial crisis of 2008 which was driven in part by opaque accounting practices related to risky assets and inadequate assessments of the financial health of key institutions. These events underlined the importance of adhering to ethical principles and ensuring transparency in financial reporting to maintain market stability and investor confidence in the future.

A study published in 2024 by the Association of Certified Fraud Examiners (ACFE) identified 1,921 cases of accounting fraud in 138 countries between 2022 and 2023, resulting in total losses of USD 3.1 billion. The study's authors categorised the fraud cases into three groups (some cases fell into more than one category, resulting in a total of more than 100%); asset misappropriation occurred in 89% of cases, with an average fraud value of USD 120,000. A total of 48% of cases were classified as corruption, with an average loss of USD 200,000, whereas the least common (5%) but most damaging in terms of financial loss (USD 776,000 per case), was financial statement fraud – an increase of 29 percentage points compared to the 2022 study data (Association of Certified Fraud Examiners [ACFE], 2024). The groups and their intersections are also illustrated in Fig. 5.1.

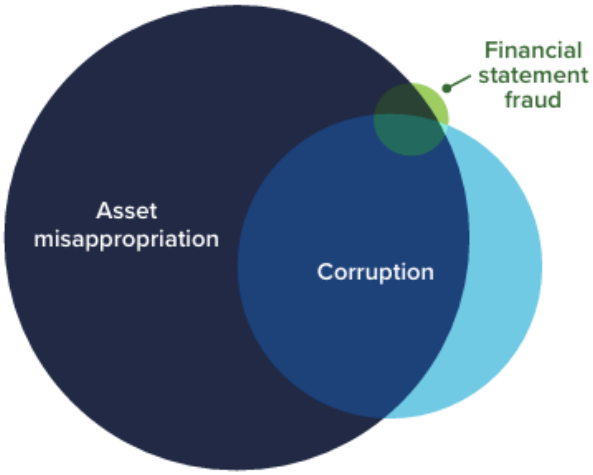


Fig. 5.1. Categorised fraud cases

Source: ACFE (2024).

When analysing who commits fraud, the authors of the study came up with some interesting findings. Managers and employees commit fraud in almost equal proportions (around 40% each), with business owners making up the remainder. However, the financial damage caused by these groups differs significantly. Employees are responsible for an average loss of USD 60,000 per case, managers USD 184,000, and owners up to USD 500,000.

The study revealed that financial statement fraud is detected relatively infrequently, yet the financial damage it causes is significantly higher than other types of fraud – more than six times greater than asset misappropriation and nearly four times greater than corruption. The fact that financial statement fraud is difficult to detect does not mean that it is rare. A review of published research on the subject suggests that creative accounting techniques, which can lead to financial statement fraud, are widely used by companies. Safta et al. (2020) found that

about 84% of Romanian companies engage in creative accounting practices. Durana et al. (2022) reported that 90% of Slovak companies used such techniques and, more recently, Blazek et al. (2023) conducted a study of companies in the V4 region and concluded that 88% of the companies in the sample used these methods.

This chapter focuses primarily on the issue of creative accounting used by entrepreneurs to manipulate financial statements and, consequently, the data presented to external stakeholders. In addition to explaining the most common applications of creative accounting, it examines the motivation behind these practices and the measures available to limit them. Academic research has developed several models to detect the use of creative accounting techniques. The author tested one of these models in an academic setting, and the concluding section presents a summary of the findings.

5.2. Creative Accounting Techniques

In examining the origins of creative accounting techniques, their emergence is generally attributed to the 20th century Anglo-Saxon economies. This development is linked to the increasing complexity of economic realities and is characterised by flexible legal frameworks that allow for subjective information in financial statements (Bachtijeva, 2021). According to Comandaru et al. (2020), the first mention of creative accounting in academic literature dates to 1976. While some view creative accounting as an innovation in financial reporting practices, it is often criticised for its potential to mislead stakeholders and undermine the transparency and reliability of financial statements, see e.g. (Kamau & Murori, 2024; Shevchenko & Liadska, 2022).

Creative accounting refers to accounting practices that, while technically legal, may be considered unethical or even fraudulent. These techniques involve the manipulation of financial data to present a company's performance in a more favourable light than reality. Although creative accounting does not always break the law, its use can result in misleading information for investors, creditors, and other stakeholders. In extreme cases, prolonged use of these techniques can mask underlying financial problems, potentially leading to severe financial distress or even corporate bankruptcy.

The most common reason for engaging in these practices is the desire to meet financial targets, which may be critical to attracting investors, maintaining shareholder confidence or securing performance-related bonuses for management. Companies may also be motivated to manipulate financial data during economic downturns to project stability and prevent market panic. Another common motivation is to inflate share value, particularly for companies preparing for mergers, acquisitions, or initial public offerings (IPOs). In such cases, the temptation to report higher profitability and lower risk – regardless of the true financial position – can be considerable.

There are various creative accounting techniques, depending on a company's specific objectives and the regulatory environment in which it operates. The most common include inflating revenues, understating expenses, deferring or accelerating income recognition, and manipulating balance sheets. While creative accounting may improve a company's short-term financial picture, it can ultimately damage its reputation, lead to regulatory penalties, or even lead to legal consequences.

Adjustments to inflate reported revenues have been extensively studied by researchers such as Gudev (2020) and Kamau and Murori (2024). Practical approaches that demonstrate the

real-world application of this technique include: early invoicing, fictitious invoicing between related parties, and upward revaluation of assets.

Early invoicing is a creative accounting method that artificially inflates revenue in the current accounting period. It involves issuing an invoice for a transaction before it actually takes place, allowing a company to report higher revenue than it should under proper accounting principles. For example, if a company signs a contract in December for the delivery of goods in January of the following year, it should correctly recognise the revenue only when the goods are actually delivered. However, if the company issues the invoice in December, it recognises the revenue early, artificially inflating its financial results for that year. While this practice may temporarily improve financial indicators, it distorts the true and fair view of the financial statements. Moreover, it creates an offsetting effect in the following period, as the company will then lack part of the revenue that should rightfully belong to the new financial year. From an accounting perspective, this practice violates the accrual accounting principle, which requires that revenues and expenses be recognised in the period in which they are incurred, regardless of when the invoice is issued or the payment is received. This manipulation can lead to a misleading improvement in financial performance, often due to pressure from shareholders or the need to meet internal targets for the reporting period.

Fictitious invoicing between related parties involves transactions where two or more financially connected entities issue invoices for services that were never provided or whose value does not reflect fair market prices. The primary objective of such transactions is to artificially inflate revenues or reduce costs, leading to the distortion of financial statements and potential tax manipulation. From an accounting perspective, such invoicing constitutes an improper increase in revenue where a company records income from non-existent transactions. In individual financial statements this can create the illusion of better financial performance than is the case. The practice is often used by management to improve financial indicators for investors, banks, or other external stakeholders, which also has significant tax implications. Fictitious invoicing between related entities can be used as a tool for tax optimisation or even tax evasion, particularly when these transactions are designed to shift profits across jurisdictions with different tax rates. This strategy, known as profit shifting, reduces the overall tax burden of a corporate group by reallocating profits to low-tax jurisdictions. For example, when a company operating in a high tax jurisdiction 'pays' a related company in a low tax jurisdiction for notional services, taxable income is effectively shifted to a more favourable tax jurisdiction. At the level of a consolidated group, these transactions have no impact on the overall financial results, as they are eliminated during preparation of the consolidated financial statements, whilst in individual companies they can have a significant impact on the calculation of tax liabilities. Due to their potential for tax abuse such practices are closely monitored by the tax authorities and regulators, implementing legislative measures to prevent their abuse.

Upward revaluation of assets increases the reported value of a company's assets. In Czechia this practice mainly applies to financial assets such as investments in securities, derivatives, or other financial instruments. Assets are revalued to fair value, which means that the book value of assets is adjusted to reflect current market prices. This process results in an increase in the value of assets on the company's balance sheet and the recognition of income, even though the company has not actually received any cash inflows. As a result, the reported increase in turnover is not the result of actual business activity, but of an accounting adjustment.

Ultimately, the same effect of an increase in the company's profits can be achieved by another common practice – understating costs in the following ways.

Deferred cost accounting is the practice of deferring the recognition of costs until the next accounting period, even though the costs relate to the previous period. This can lead to an artificial improvement in profit for the year because costs that should reduce profit are deferred and recognised later. For example, if a company uses external services (such as consulting, marketing, or IT support) in December but receives the invoice in January, the correct accounting treatment would be to recognise the expense in the previous year. However, if the company recognises it in the new accounting period, it effectively reduces the previous year's expense, thereby inflating reported profits while shifting the financial impact to the following year. This practice was observed in the case of Czech Airlines, which recognised aircraft lease payments in later periods than when they were actually made.

Capitalisation is the **reclassification of current operating expenses as capital expenditure**, allowing them to be amortised over future periods rather than being expensed immediately. This approach can temporarily improve financial results by reducing total expenses in the reported period below their actual level. A common example is the classification of development costs. A company needs to determine whether such costs should be treated as current operating expenses, which should be recognised immediately, or as capitalisable investments that are expected to generate future economic benefits. If an enterprise recognises expenditure on developing a new technology as a long-term intangible asset rather than as an expense, its current profit will appear higher.

Companies can **manipulate the depreciation period** to artificially reduce annual expenses and increase reported profits. This occurs when a company extends the depreciation schedule beyond the recommended useful life of an asset, thereby reducing annual depreciation costs and temporarily improving financial performance. For example, consider a new manufacturing machine with a recommended useful life of 10 years, which means it should be depreciated over that period. If the company decides instead to depreciate it over 20 years, the annual depreciation expense is effectively halved. As a result, reported expenses for the first ten years are lower than they should be, artificially inflating profits and creating a distorted view of the company's financial health.

Ignoring the principle of prudence in accounting is a fundamental accounting concept that ensures a true and fair view of a company's financial position. Under this principle, companies are required to make provisions and allowances to reflect potential risks and future losses. If a company fails to recognise these items or deliberately under-recognises them, it artificially improves its financial results and gives a misleading picture of its economic health. Allowances are made to reduce the book value of assets when there is a risk that the company will not recover their full value. A common example is the creation of allowances for doubtful accounts. If a company does not make such adjustments, it reports higher asset values on its balance sheet, even though some of these assets may be uncollectible. Adherence to the principle of prudence is essential for accurate financial reporting and for the long-term stability of the company. Failure to make provisions and allowances may temporarily improve reported profits, but it significantly increases the risk of financial difficulties in the future.

Most of the profit adjustments mentioned above also have an impact on the balance sheet, both indirectly (as net profit is part of equity on the liabilities side) and directly, as listed below:

- **Overstatement of fixed assets** – the revaluation of assets, the classification of expenditure as capital expenditure and the extension of depreciation periods results in the overstatement of fixed assets.

- **Higher value of receivables** – early or fictitious invoicing and the absence of impairment provisions result in receivables being reported at a higher value than their actual recoverable amount.
- **Understatement of liabilities** – delayed recognition of invoices received or failure to make provisions leads to an understatement of the company's actual liabilities.

All of these practices make a company appear to external stakeholders to be financially healthier and more stable than it actually is. Artificially inflating revenues, understating expenses, overstating assets or manipulating liabilities results in financial statements that do not present a true and fair view of the company's performance – one of the core principles of financial reporting. Such a company will report higher profitability, which may influence the decisions of investors, creditors and business partners. Higher profits can give the impression that the company is profitable and less risky, making it easier to obtain loans, investments or favourable contracts. Similarly, reporting higher asset values can increase the company's market value and attractiveness to capital markets. For example, if a company reports inflated asset values, this can lead to an overvaluation of its shares, which poses a significant risk to investors who rely on this information to make decisions. Reporting lower liabilities can distort the true level of the company's indebtedness and solvency. A company that appears to have fewer liabilities may appear more financially stable and thus obtain better credit terms or more favourable contracts. The creators of such manipulations not only violate ethical accounting principles, but also risk legal consequences when they cross the line between creative accounting and accounting fraud. Accounting ethics emphasises that financial statements should give a true and fair view of the financial position of a company (Remenarić et al., 2018). This principle is further supported by the International Federation of Accountants (IFAC), which has issued a code of ethical conduct for accountants that outlines five fundamental principles that every accountant should uphold:

- **Integrity** requires for the accountant to act honestly and fairly in all professional and business relationships.
- **Objectivity** is focused on avoiding bias and conflicts of interest, and emphasises that accountants should resist pressure from individuals or entities seeking to manipulate accounting data.
- **Professional Competence & Due Care** – accountants are required to maintain their professional knowledge and skills at a level that ensures they remain competent and able to apply relevant laws and professional standards effectively.
- **Confidentiality** means that information obtained during professional and business relationships shall remain confidential and shall not be disclosed to others without proper authority.
- **Professional Behaviour** – accountants must comply with laws and regulations, act in the public interest, and avoid any conduct that may bring the accounting profession into disrepute.

5.3. Creative Accounting Motives

Motives for creative accounting can vary but often include the pursuit of personal and/or corporate goals, such as meeting financial targets or increasing share prices. These actions can result in significant financial losses to stakeholders and damage the reputation of the accounting profession (Kaaya, 2022).

From a personal motivation perspective, the most common driver is often a managerial bonus, whether in the form of salary-based rewards or the promise of employee stock options, linked to the company's profit performance. As a result, managers may be incentivised to manipulate financial statements to achieve the desired figures for their personal benefit. Other motives usually lead to the achievement of business objectives and may include: improving the financial picture for investors, improving the financial picture for banks, lenders or customers, tax optimisation.

Improving the financial picture for investors – the motivation for creative accounting is often driven by management's desire to demonstrate continued profit growth and thereby present strong financial results to external stakeholders. A notable example of a company whose management used such techniques in the early 2000s is WorldCom. Investigations revealed that the first accounting manipulations occurred around mid-1999. The most significant adjustment identified was the reclassification of operating expenses as long-term capital expenditures, specifically when the costs of maintaining telecommunications networks were recorded as capital assets. These accounting manipulations went undetected for three years, eventually uncovering adjustments totalling USD 11 billion. As a result of the company's collapse, shareholders lost approximately USD 180 billion (Al-Dulemi & Al-Shabatat, 2018).

Improving the financial picture for banks, lenders or customers is closely related to the previous one but focuses on management's efforts to achieve accounting figures required by banks to secure more favourable loan terms or to obtain additional funding. Similar behaviour is often observed among creditors who may be unwilling to provide assets or services on trade credit without satisfactory financial indicators – Enron was a prime example of this. The company's management improved its financial position by prematurely recognising revenue on contracts for future supplies of energy or services that had not yet materialised, and secondly by hiding debt and expenses through the use of special purpose entities (SPEs). Enron hid debts and costs outside of its main financial statements. Unsuccessful investments were also similarly kept off Enron's balance sheet. As a result of these manipulative practices, shareholders lost USD 74 billion in the four years leading up to the company's bankruptcy (Al-Dulemi & Al-Shabatat, 2018). In Czechia, an improvement of financial results was observed in the case of Skanska, which artificially inflated its profits in the Třinec division by about CZK 500 million over three years (Matocha, 2006).

Tax optimisation means that to reduce tax liability, company management may set up subsidiaries in tax havens. Through fictitious invoicing, profits are shifted to these jurisdictions, thereby reducing the overall tax burden for the entire corporate group. This practice was examined by Tørsløv et al. (2022), who identified Ireland as the largest tax haven in the EU. In 2015, foreign companies shifted around USD 100 billion in profits to Ireland – more than to any Caribbean country.

In addition to the two companies mentioned above, Parmalat and Tesco also used these motives and practices.

5.4. Creative Accounting – Prevention by a Company

To minimise the potential use of creative accounting techniques, companies should prioritise maximum transparency and integrity in financial reporting. This includes implementing internal controls, promoting and enforcing ethical standards, and complying with regulatory frameworks. While some of these measures can be addressed internally by the company,

others require educational involvement both through primary education (e.g. schools) and lifelong learning (e.g. professional training and courses). In more serious cases, solutions may involve legislative adjustments and the implementation of related restrictions. The different areas of prevention can be divided into: internal controls, external control, code of ethics and culture, strict compliance with accounting standards.

Internal controls is the simplest way to defend against potential fraud within a company. Responsibility should be divided among several people to ensure that no person has complete control over the company's accounting, for example by the introduction of dual approval for significant payments. In line with the previous point (although it may seem contradictory), it is crucial to establish clear rules defining the authority of each position, particularly regarding access rights within accounting software and the ability to modify records. Such a system should be complemented by internal audits and spot checks, which can identify discrepancies at an early stage and prevent potential damage. Osmanović and Šarić (2023) conducted research among companies in Bosnia and Herzegovina and came to similar conclusions. Their survey confirmed that adequate control procedures either prevent fraud or detect it quickly enough to prevent its continuation. Such results were found in an earlier study conducted in the neighbouring Serbia (Ćerdić & Knežević, 2021).

External control is more financially demanding on the company than the previous method. However, a key advantage is that those performing the control are less likely to fear job loss (due to potential disapproval from management) if they uncover problems or fraud, which can be a weakness of internal audit. External control, most commonly in the form of an external audit, provides an independent review of the financial statements, thereby minimising the risk of manipulation. To enhance the credibility of such audits, it is recommended that auditors or audit firms be rotated regularly to avoid the development of close relationships between the auditor and the audited entity. Transparency is further enhanced when the audit report is presented to the owners and not only to management. In cases of uncertainty, it is advisable to proceed with a more in-depth audit focused on the identified concerns. Shah (1998) examined this area in the context of British companies, and concluded that auditors enhance the reliability of financial statements and are expected to actively verify compliance with the principle of providing a true and fair view.

Code of ethics and culture as a preventive measure should be seen in a long-term context, as it requires changing the mindset not only of employees, but of society, to ensure that everyone understands that manipulating financial statements is unethical. Within a company, it is important not to put pressure on employees, ideally implementing a corporate code of ethics that sets out the principles to which employees must adhere to. Regular ethics training should be provided, emphasising both the legal and professional consequences of accounting fraud. Best practice is for management to lead by example and avoid pressuring subordinates to alter financial results (for example, through bonus schemes linked to the achievement of specific financial targets), a concern highlighted by Roy and Choudhary (2016). Focusing on accounting students, Hermawan et al. (2023) found that early exposure to the ethics of the accounting profession and issues surrounding creative accounting positively influenced future behaviour. Similar findings were obtained by Christensen et al. (2018) and Okougbo and Okike (2021), highlighting the importance of ethics education in shaping responsible financial practices.

Strict compliance with accounting standards means it is essential that internal policies set out precise procedures that must be strictly adhered to, and it is not important whether these rules are based on national legislation, International Financial Reporting Standards (IFRS) or US

Generally Accepted Accounting Principles (US GAAP). The aim is to minimise the possibility of creative accounting adjustments by employees or management. As part of these procedures it is crucial to increase transparency for external stakeholders regarding changes within the company. In Czechia such practices should be implemented through notes to the financial statements, where companies are expected to provide a detailed explanation of the accounting methods they use, how changes in financial reporting occur, and the reasons for these changes. A currently voluntary, yet credibility enhancing practice, is the disclosure of non-financial information about the company, e.g. Tesla, which publishes quarterly reports on the number of vehicles produced and delivered.

5.5. Creative Accounting – Fraud Detection

When internal prevention systems fail, it is necessary to implement fraud detection methods. In recent years the development of artificial intelligence has made it possible to integrate automated processes into accounting systems that detect suspicious behaviour (e.g. non--compliance with internal policies) and notify the appropriate personnel for further investigation. Artificial intelligence can be more effective at identifying patterns of behaviour that might go unnoticed by humans, particularly due to the large amount of data that needs to be analysed, as noted by Ali et al. (2024). Examples of such detection techniques include recurring payments to the same entities or identical bank account numbers used by both employees and suppliers.

Another approach is forensic accounting, which increasingly integrates techniques such as data mining, blockchain, and cybersecurity, as highlighted by Haddad et al. (2024). These techniques not only analyse historical data but also prevent retrospective changes to accounting records, processing both structured (e.g. numerical figures and invoices) and unstructured data (e.g. contracts and emails) to detect anomalies. Using advanced tools and software (such as Power BI), these methods can uncover complex and suspicious relationships and identify irregularities hidden in financial data.

5.6. Creative Accounting – Academic Research

The above methods are primarily designed for companies and their internal staff or management. However, when considering the issue from the perspective of external users, different approaches need to be adopted. This is mainly due to the limited access to primary accounting data that would otherwise allow the identification of irregular or manipulative practices. In academic research, several approaches have been developed to detect irregular financial behaviour based on publicly available information.

In Central Europe, four models are commonly used to analyse creative accounting practices. The CFEBT model was developed specifically for companies in Czechia, but has already been tested on Slovak companies. This method analyses the development of cash flow (CF) and earnings before tax (EBT) (Kovalová & Frajtová Michalíková, 2020), using the formula:

$$\mathrm{CFEBT} = \sum_{t=1}^{5} \left(\frac{\Delta \mathrm{CF}_t - \mathrm{EBT}_t}{\mathrm{EBT}_t} \right).$$

When the CFEBT exceeds the materiality threshold (typically 5-10%), there is an increased risk of distorting the true and fair view of financial reality. In such cases, it is necessary to analyse significant discrepancies between cash flows and financial performance, as these discrepancies may be caused by significant corporate investments.

The next method used to identify creative accounting is the Jones model and its variants. More details can be found in (Durana et al., 2022):

$$\frac{\mathrm{NDA}_{it}}{\mathrm{A}_{it-1}} = \alpha_0 \frac{1}{\mathrm{A}_{it-1}} + \alpha_1 \frac{\Delta\mathrm{REV}_{it} - \Delta\mathrm{REC}_{it}}{\mathrm{A}_{it-1}} + \alpha_2 \frac{\mathrm{PPE}_{it}}{\mathrm{A}_{it-1}} + \varepsilon_{it},$$

where: NDA_{it} – non-discretionary accrual in year *t*,
TA_{it} – total accrual in year *t*,
A_{it-1} – total assets in year *t*–1,
$\Delta\mathrm{REV}_{it}$ – annual change in revenue in year *t*,
$\Delta\mathrm{REC}_{it}$ – annual change in receivables in year *t*,
PPE_{it} – long-term tangible assets in year *t*,
α_0, α_1, α_2 – coefficients,
ε_{it} – prediction error.

The last two models were developed by Beneish, who established the standard 5-parameter model and later extended it to the 8-parameter model (Durana et al., 2022). The formula for the first model is:

M-Score = –6.065 + 0.823 × DSRI + 0.906 × GMI + 0.593 × AQI + 0.717 × SGI + 0.107 × DEPI.

The formula for the 8-parameter model is:

M-Score = –4.84 + 0.92 × DSRI + 0.528 × GMI + 0.404 × AQI + 0.892 × SGI + 0.115 × DEPI – 0.172 × SGAI + 4.679 × TATA – 0.327 × LVGI,

where: DSRI – days' sales in a receivable index,
GMI – gross margin index,
AQI – asset quality index,
SGI – sales growth index,
DEPI – depreciation index,
SGAI – sales, general and administrative expenses index,
LVGI – leverage index,
TATA – total accruals to total assets.

The classification rule for these models was set by Beneish at –2.22, which is the boundary between manipulation and non-manipulation. If the resulting M-score is below this value, there has been no manipulation of the financial statements in the accounting period.

Beneish (1999), the author of the two models mentioned above, justifies each financial ratio and its evolution over time as follows:

- DSRI – measures the year-on-year change in receivables relative to sales. An increase in the DSRI may indicate a change in credit policy or an excessive increase in receivables relative to sales, increasing the likelihood of overstatement of sales.
- GMI – a decline in gross margin worsens a company's outlook. Beneish hypothesised a positive relationship between GMI and earnings manipulation.

- AQI – a value greater than 1 indicates deferred expense recognition (e.g. suspension of depreciation). There is a positive relationship between AQI and earnings manipulation.
- SGI – high sales growth may indicate manipulation to achieve targeted earnings. A positive correlation is expected between SGI and earnings manipulation.
- DEPI – a value above 1 indicates an extension of the useful life of assets. A positive relationship with earnings manipulation is expected.
- SGAI – increasing SGA expenses relative to sales may signal a negative outlook. A positive relationship with earnings manipulation is expected.
- LVGI – a value above 1 indicates increasing financial leverage, often linked to debt covenants.
- TATA – a higher level of accruals signals a greater likelihood of earnings manipulation.

As most of the indicators are based on year-on-year changes, Beneish (1999) ensured that the data did not have extreme values by applying winsorisation at the 1% level to both tails.

If a particular variable was missing from the calculation (i.e. had a value of zero), the ratio was automatically replaced by 1 (neutral value) – this applied to AQI, DEPI, and SGAI. This assumption implies that Beneish considered a neutral benchmark value of 1 for each financial ratio. If a value exceeded this threshold, it was flagged as a potential indicator of earnings manipulation.

However, subsequent research using Beneish's models did not fully agree with this assumption, and thresholds for individual indicators have evolved. For example, Durana et al. (2022) set updated thresholds based on their empirical findings, as shown in Table 5.1.

Table 5.1. Cut-off scores for each indicator

DSRI	GMI	AQI	SGI	DEPI	SGAI	LVGI	TATA
≥ 1.46	≥ 1.19	≥ 1.25	≥ 1.61	≥ 1.077	≥ 1.041	≥ 1.111	≥0.031

Source: own processing based on (Durana et al., 2022).

Srbová and Pěta (2024) examined Czech companies with total assets of up to CZK 500 million and with annual turnover of up to CZK 1 billion. The dataset included only companies with complete financial statements for all the analysed years 2016-2018, providing a database of 4,515 companies.

The analysis showed that 74.33% of these companies used creative accounting practices to manipulate their financial results during the observed period, whilst 26.51% used these techniques consistently throughout the period, meaning that their financial statements showed signs of accounting manipulation. This distorts the true financial picture of the company.

The research compared these findings with the cut-off values for each indicator, as established by Durana et al. (2022). Table 5.2 presents the results of creative accounting practices based on the sub-criteria of the two evaluation approaches.

Table 5.2. Percentage of companies that exceed cut-off values – comparing two approaches

DSRI	GMI	AQI	SGI	DEPI	SGAI	LVGI	TATA	Approaches' authors
67.20	63.34	26.45	81.97	40.11	71.56	66.93	2.39	Beneish (1999)

31.87	49.94	16.39	17.21	31.85	67.13	42.83	81.44	Durana et al. (2022)

Source: (Srbová & Pěta, 2024).

There were significant differences in the identification of adjusted data depending on the specific indicators used. For example, while Durana et al. (2022) set a cut-off value of 1.61 for the sales growth index, Beneish (1999) consistently used a threshold of 1. In contrast, for the total accruals to total assets indicator, Durana et al. (2022) suggested that values above 0.031 indicate potential data manipulation, which differs from Beneish's method.

5.7. Conclusions

In general, the use of creative accounting techniques poses significant challenges and risks for all stakeholders. While the manipulation of financial statements may appear to provide a competitive advantage, in reality it has long-term negative consequences that can threaten the financial stability, credibility and even the very existence of a company. Business that engage in creative accounting run the risk of asset loss and financial instability. The distorted financial results can lead to a misallocation of resources, resulting in unsustainable financial decisions. If the legal threshold is crossed, companies may face heavy fines, lawsuits, or even criminal prosecution of those responsible. In addition, those that manipulate their financial statements may gain an unfair advantage over businesses that comply with accounting standards, thereby distorting market competition. In extreme cases, accounting scandals can lead to wider economic disruption, affecting not only individual companies but entire sectors and economies.

Creative accounting harms not only the company itself, but also external entities that rely on distorted financial information to make critical decisions. The negative effects also extend to public finances. If a company overstates expenses in a high-tax jurisdiction or inflates profits in low-tax jurisdictions, it can artificially reduce its tax liability, ultimately resulting in lower revenues for the state budget.

In addition to traditional approaches, modern technologies that were previously unavailable can now be used. The key advantage of these new tools is their efficiency, particularly in handling large volumes of data, which these methods can effectively process and analyse. When it comes to evaluating financial data from an external perspective, a study by Srbová and Pěta (2024) suggested that most companies in Czechia use some form of creative accounting techniques. More worrying findings were reported by Durana et al. (2022), who found that only 1 in 10 companies refrained from using such methods, indicating a widespread problem in financial reporting practices.

References

Ali, A. M., Khinger, I. K., Subhe, A., & Al-Orfali, A. K. (2024). Forensic Accounting Techniques in Detecting Frauds. *Journal of Ecohumanism*, *3*(5), 543-558. https://doi.org/10.62754/joe.v3i5.3922

Al-Dulemi, K. I., & Al-Shabatat, I. O. A. (2018). The Impact of Corporate Governance Tools in the Reduction of Creative Accounting Practices in the Jordanian Commercial Banks. *Research Journal of Finance and Accounting*, *9*(16), 1-15.

Association of Certified Fraud Examiners [ACFE]. (2024). *Occupational Fraud 2024: A Report to the Nations*. https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2024/2024-report-to-the-nations.pdf

Bachtijeva, D. (2021). Can Creative Accounting Be Equated with Creativity and Called Positive? *Buhalterinės apskaitos teorija ir praktika*, (24), 3. https://doi.org/10.15388/batp.2021.37

Beneish, M. D. (1999). The Detection of Earnings Manipulation. *Financial Analysts Journal*, *55*(5), 24-36. https://doi.org/10.2469/faj.v55.n5.2296

Blazek, R., Durana, P., & Michulek, J. (2023). Renaissance of Creative Accounting Due to the Pandemic: New Patterns Explored by Correspondence Analysis. *Stats*, *6*(1), 411-430. https://doi.org/10.3390/stats6010025

Ćerdić, I., & Knežević, G. (2021). The Emergence of Creative Accounting in Insufficiently Regulated Business Systems. In *Proceedings of the 8th International Scientific Conference – FINIZ 2021* (pp. 58-64). https://doi.org/10.15308/finiz-2021-58-64

Christensen, A., Cote, J., & Latham, C. K. (2018). Developing Ethical Confidence: The Impact of Action-Oriented Ethics Instruction in an Accounting Curriculum. *Journal of Business Ethics*, *153*(4), 1157-1175. https://doi.org/10.1007/s10551-016-3411-4

Comandaru, A.-M. A., Stanescu, S.-G., Toma, C. M., & Paduraru, A. H. (2020). Another Image of Accounting – Creative Accounting. *Global Journal of Business, Economics and Management: Current Issues*, *10*(2), 100-110. https://doi.org/10.18844/gjbem.v10i2.4695

Directive 2006/43/EC of the European Parliament and of the Council of 17 May 2006 on Statutory Audits of Annual Accounts and Consolidated Accounts, Amending Council Directives 78/660/EEC and 83/349/EEC and Repealing Council Directive 84/253/EEC (Text with EEA relevance). *OJ* L 157, 9.6.2006, pp. 87-107.

Durana, P., Blazek, R., Machova, V., & Krasnan, M. (2022). The Use of Beneish M-Scores to Reveal Creative Accounting: Evidence from Slovakia. *Equilibrium. Quarterly Journal of Economics and Economic Policy*, *17*(2), 481-510. https://doi.org/10.24136/eq.2022.017

Gudev, I. (2020). Creative Accounting – Definition, Types, Purposes and Impact on United Nations' Sustainable Development Goals. *Economic Alternatives*, (2), 328-341. https://doi.org/10.37075/EA.2020.2.09

Haddad, H., Alharasis, E. E., Fraij, J., & Al-Ramahi, N. M. (2024). How Do Innovative Improvements in Forensic Accounting and Its Related Technologies Sweeten Fraud Investigation and Prevention? *WSEAS Transactions on Business and Economics*, *21*, 1115-1141. https://doi.org/10.37394/23207.2024.21.93

Hermawan, S., Nadiroh, P., Rahmawati, I. D., Qonitah, I., Lating, A. I. S., & Alieva, S. S. (2023). Professional Ethics and Ethical Orientation: Key to Preventing Creative Accounting Practices Among Accounting Students. In *Proceedings of the International Conference on Intellectuals' Global Responsibility (ICIGR 2022)* (pp. 593-599). https://doi.org/10.2991/978-2-38476-052-7_65

Kaaya, I. D. (2022). Motives and Ethics of Creative Accounting: A Reflective Review and Views. *African Journal of Accounting and Social Science Studies*, *4*(1), 315-343. https://doi.org/10.4314/ajasss.v4i1.17

Kamau, C. G., & Murori, C. K. (2024). Characteristics of Creative Accounting: A Multifaceted Literature Analysis. *World Journal of Advanced Research and Reviews*, *23*(1), 2035-2043. https://doi.org/10.30574/wjarr.2024.23.1.2177

Kovalová, E., & Frajtová Michalíková, K. (2020). The Creative Accounting in Determining the Bankruptcy of Business Corporation. *SHS Web of Conferences*, *74*, Article 01017. https://doi.org/10.1051/shsconf/20207401017

Matocha, P. (2006). Půlmiliardový podvod: Skanska. *EURO*, *(15)*48. https://www.euro.cz/clanky/pulmiliardovy-podvod-793407/

Okougbo, P. O., Okike, E. N., & Amoo, E. O. (2021). Teaching Strategies in Accounting Ethics: A Students' Assessment of Preferred Teaching Styles. *Cogent Social Sciences*, *7*(1), 10. https://doi.org/10.1080/23311886.2021.1950306

Osmanović, A., & Šarić, D. (2023). Importance of Internal Control for Creative Accounting. *Agora International Journal of Economic Sciences*, *17*(1), 93-101. https://doi.org/10.15837/aijes.v17i1.5766

Remenarić, B., Kenfelja, I., & Mijoč, I. (2018). Creative Accounting – Motives, Techniques and Possibilities of Prevention. *Ekonomski vjesnik*, *31*(1), 193-199.

Roy, T., & Choudhary, D. R. (2016). Creative Accounting: A Tool to Suit Whims of the Top Management. *Review*

of Professional Management – A Journal of New Delhi Institute of Management, *14*(1), 69-74. https://doi.org/10.20968/rpm/2016/v14/i1/109409

Safta, I.-L., Achim, M. V., & Borlea, S. N. (2020). Manipulation of Financial Statements Through the Use of Creative Accounting. Case of Romanian Companies. *Studia Universitatis „Vasile Goldis" Arad – Economics Series*, *30*(3), 90-107. https://doi.org/10.2478/sues-2020-0019

Shah, A. K. (1998). Exploring the Influences and Constraints on Creative Accounting in the United Kingdom. *European Accounting Review*, *7*(1), 83-104. https://doi.org/10.1080/096381898336592

Shevchenko, L., & Liadska, V. (2022). The Essence of Creative Accounting. *Economics. Finances. Law*, (6), 24-26. https://doi.org/10.37634/efp.2022.6.5

Srbová, P. & Pěta, J. (2024). Creative Accounting Practices: Literature Review and Results from Czech SMEs. *Globalizacia*.

Tørsløv, T., Wier, L., & Zucman, G. (2023). The missing profits of nations. *The Review of Economic Studies*, *90*(3), 1499-1534. https://doi.org/10.1093/restud/rdac049

Chapter 6

Blocking of Bank Accounts by the National Revenue Administration

Michał Biernacki

Wroclaw University of Economics and Business
ORCID: 0000-0002-7269-8212

Quote as: Biernacki, M. (2025). Blocking of Bank Accounts by the National Revenue Administration. In I. Chuy, P. Luty, V. Lakatos (Eds.), *Modern Tools for Fraud Detection: Insights from the V4 and Ukraine* (pp. 76-84). Publishing House of Wroclaw University of Economics and Business.

DOI: 10.15611/2025.40.5.06

6.1. Introduction

The proper and stable functioning of the state budget system, and thereby the security of public finances, is primarily achieved through the implementation of solutions that may not always be popular but enable the reduction of the shadow economy and tax fraud. Advanced solutions and their implementation increase the level of security and enhance fiscal efficiency, however they also define the predictability of tax relations between the state and taxpayers, ensuring an acceptable level of tax burdens while maintaining taxpayer trust in the state.

The purpose of this chapter was to present the procedures for bank account blocking by the National Revenue Administration (Krajowa Administracja Skarbowa – KAS), aiming to secure public-law liabilities, including tax obligations. This chapter outlines the reasons, the process, and the consequences of such a blockade.

A bank account blockade by KAS can occur in various circumstances, most often when a taxpayer fails to pay their tax on time, has outstanding social security contributions, or is subject to enforcement proceedings. It is also necessary to consider whether such actions by the tax authorities may hinder business financial management, generate additional costs for the taxpayer, and lead to a loss of trust between taxpayers and the state.

To achieve this objective, it was necessary to systematise the possibilities and procedures for bank account blocking by the National Revenue Administration, identify the procedures, and analyse and present court rulings. The main research methods used included legal analysis, deduction, and critical analysis.

6.2. Preliminary Assumptions

The blocking of bank accounts in business practice is a frequently used measure even at the stage prior to the initiation of criminal or administrative proceedings. Once blocked, the bank account holder cannot freely use and dispose of the blocked funds, withdraw or transfer them to another account. This can lead to difficulties in paying off tax liabilities, contractual obligations or other debts, generating additional and new problems for the bank account holder.

The blocking of bank accounts by the National Revenue Administration is an issue that has recently attracted much controversy and doubt among the public. The decision to block bank accounts in many cases has serious consequences for those affected, so it is important to have a correct understanding of the procedures and rights involved.

The monitoring of bank accounts by the so-called 'treasury' is understandable in the case of entrepreneurs, as can be deduced from the opinions expressed by Poles, particularly when it comes to the 'VAT mafia' aspect. Nowadays, standard VAT carousels are largely a thing of the past, as the introduction of JPK_VAT (Uniform Control File_VAT) has significantly curbed this practice. Ongoing VAT problems have become more sophisticated and nuanced, making them more difficult to detect. In terms of losses to the Treasury, the main problem at present appears to be the so-called grey market. The blocking of a bank account can take place on two legal levels: the tax ordinance as well as banking law.

6.3. Blocking of Bank Accounts Based on the Tax Ordinance

The National Revenue Administration can block the accounts of entities suspected of using the banking sector for tax evasion for up to 72 hours, which can be extended up to three months. Note that the grounds for its application do not have to be proven – it is sufficient to make them plausible.

The use of blocking is employed to counteract the use of the financial sector for tax evasion, especially in the field of VAT. The indication to reach for this solution is mainly the result of the analysis of the STIR system (Teleinformatic Clearing House System) processing data provided by banks and SKOKs (Stefczyk's Bank – Cooperative Savings and Credit Bank). The analysis covers information on transactions on accounts of so-called qualified entities, i.e. natural persons who are entrepreneurs, natural persons who do not have the status of entrepreneurs, but who carry out gainful activity on their own account, legal persons and organisational units without legal personality, but which have legal capacity. Bank settlement accounts, time deposits, accounts held for business purposes with SKOKs and VAT accounts of these entities are monitored. The fraud risk index qualifying blocking is determined for a given entity based on algorithms developed by the clearing house. The algorithms, by definition, take into account the best practices of banks and SKOKs in preventing their use for criminal activities, as well as economic, geographical or subject matter criteria pursuant to Article 199 zn § 3 points 1-5 of the Tax Ordinance (Ustawa z dnia 29 sierpnia 1997…). The collected information on the risk indicator is received by the Head of KAS.

As already indicated, the blocking is applied for a period of not more than 72 hours, but may be extended for a specified period of time not exceeding three months. Short account blocking occurs when information received indicates that a qualified entity may be using financial sector

activities for purposes related to tax evasion or for activities aimed at tax evasion, and is a countermeasure here. Its function is to immediately interrupt a suspicious transfer of money in accordance with Article 119zv § 1 of the Tax Ordinance (Ustawa z dnia 29 sierpnia 1997…). Fiscal extortion and activities aiming at it do not have to occur directly in a qualified entity. According to the judgment of the Supreme Administrative Court of 3 June 2022 (Wyrok NSA z dnia 3 czerwca 2022…), tax fraud may also be perpetrated by another entity, but if a qualified entity uses the activities of banks or SKOKs for the purposes of this fraud, the blocking of its account may be necessary to counteract tax fraud by another entity. An extension of the blocking occurs when there is a reasonable fear that the qualified entity will not fulfil an existing, or about to arise, tax or third-party tax liability obligation exceeding the equivalent of EUR 10,000. Conversion into zlotys is made according to the average euro exchange rate announced by the National Bank of Poland on the last working day of the year preceding the year in which the decision to extend the blockade was made (Ustawa z dnia 29 sierpnia 1997…, Art. 119zw § 1).

The assessment of whether it is necessary to extend the blocking of the account should be made in accordance with the rules applicable to the establishment of security for the payment of tax liabilities. The rationale for the application of both solutions is a well-founded fear of non-performance of the tax liability. The purpose of blocking the account is to secure funds that should be used to pay the tax due, before they are transferred outside the Polish banking system. The circumstances justifying the application are: failure to settle an existing tax liability, relatively low income of the taxpayer in relation to the future tax liability or failure to disclose the value of supplies and acquisitions (Wyrok NSA z dnia 16 lutego 2022…).

The bank account may be blocked, pursuant to Article 119zg point 4 and point 5 of the Tax Ordinance Act (Ustawa z dnia 29 sierpnia 1997…), when:

1) natural persons who are entrepreneurs (including farmers who are considered entrepreneurs according to the judgment of the Supreme Court (Wyrok SN z dnia 3 października 2014…) and Supreme Court resolution (Uchwała SN z dnia 26 lutego 2015…);
2) natural persons conducting a gainful activity for their own account who are not entrepreneurs, e.g. persons who achieve the so-called income from activities pursued personally listed in Article 13 of the Personal Income Tax Act (Ustawa z dnia 26 lipca 1991…), such as income of contractors, managers, members of management boards, supervisory boards, auditing committees and other governing bodies of legal persons;
3) legal persons, e.g. limited liability companies, joint stock companies, cooperatives, state-owned enterprises, foundations, registered associations;
4) organisational entities without legal personality but with legal capacity, e.g.:
    a) general partnerships, limited partnerships, limited joint-stock partnerships, housing communities,
    b) limited liability companies and joint-stock companies in organisation, regular associations.

Those whose accounts are blocked have little chance of successfully challenging this action.

A short blockade takes the form of a demand communicated to the bank or SKOK, and it is not subject to a legal remedy in its own right. An extension of the blockade, on the other hand, requires a ruling. The entrepreneur may file a complaint. Once the complaint procedure has been exhausted, the decision can be appealed to the administrative court. It should be noted that the accepted position is that in a complaint or an action against the decision on the extension of the account blockade, the reasons for its application (making a short blockade)

may also be challenged. Indeed, the two blockades are interrelated. The KAS, when making a (short) blockade, does not have to prove the use of the financial sector by the entity in question for tax evasion. It only has to prove that such a probability exists. This means that it must present the view that criminal activities may have occurred or may occur in the future. It should be noted that all actions of the Head of the KAS are discretionary in nature. When the Head of KAS finds that the reason for the blockade has ceased during the extension of the blockade period, he/she is obliged to revoke the blockade.

According to the judgment of the Supreme Administrative Court (Wyrok NSA z dnia 26 stycznia 2022…), the key evidence in the case is the risk analysis made in STIR. Determining exactly who was committing tax evasion, in what manner and to what scale is not within the scope of account blocking proceedings, and especially within the framework of proceedings preceding a short block. The final assessment of the correctness of the suspected entity's accounts only takes place in the course of an audit or tax proceedings, and as a result of this verification, it may turn out that it has nevertheless acted lawfully.

The order extending the blockade must be issued within three days. This excludes the conduct of proceedings with a classic evidentiary procedure, ensuring the qualified entity's active participation in it, setting a deadline for reading the case file. It should be noted that it is unrealistic to take explanations from the trader or to interview witnesses. The authority does not conduct evidentiary proceedings to the same extent as in tax assessment proceedings, but assesses the circumstances related to the performance of the disputed transactions taking into account the evidence collected in the course of checking activities, inspections or tax proceedings or resulting from tax returns and JPK_VAT files.

Within the framework of the procedure for challenging the blocking of a bank account, the correctness of the findings of the tax authorities as final and binding for the determination of the tax liability is not assessed, but only examined whether the circumstances given by the tax authority justify the application of such blocking, i.e. whether the authority has substantiated the premises for blocking the bank account. It should be noted that it is problematic whether it is possible to challenge the blocking of an account made for 72 hours; in this respect, one may observe discrepancies in court judgments. The Provincial Administrative Court in Warsaw stated that the proceedings on a short (72-hour) blockade and the proceedings on the extension of the blockade, although they must overlap in time, operate on completely different premises, and the contestability is provided for only in the later procedure (Wyrok WSA z 10 kwietnia 2020…). On the other hand, the judgment of the Supreme Administrative Court specifies that the interpretation and analysis of the content of the provisions of the Tax Ordinance, consistent with the constitutional principles, leads to the conclusion that the prerequisites of a short blockade of an account are subject to judicial and administrative control in the case of challenging the decision of the Head of the KAS on the extension of such blockade for a specified period (Wyrok NSA z 27 kwietnia 2020…). When considering the constitutional norms, one should follow the second of the presented views and indicate that both the initial blockade and its extension are subject to judicial-administrative control. One has to agree with the position that in a complaint against an order extending a blockade (and in a court action) it is possible to challenge the making of a 72-hour blockade. In summary, it can be stated that challenging the blocking of a bank account under the STIR is done by means of a complaint and a complaint to an administrative court. Both the establishment of a short blockade and its extension can be challenged in the legal remedies.

According to the STIR regulations, fiscal extortion is:

- fiscal offences
  - tax evasion (Ustawa z dnia 10 września 1999…, Art. 54 § 1 and 2),
  - *firmanctwo* (Ustawa z dnia 10 września 1999…, Art. 55 § 1 and 2), i.e. fraudulently conducting business activity under the name of another person or company,
  - tax fraud (Ustawa z dnia 10 września 1999…, Art. 56 § 1 and 2),
  - failure to issue, issuing defectively or refusing to issue an invoice or bill (Ustawa z dnia 10 września 1999…, Art. 62 § 1),
  - issuing or using an untrustworthy invoice or bill (Ustawa z dnia 10 września 1999…, Art. 62 § 2 and 2a),
  - defrauding of an overpayment or refund of tax (Ustawa z dnia 10 września 1999…, Art. 76 § 1 and 2);
- crimes:
  - forgery or falsification of an invoice or the use of such an invoice as authentic according to the Penal Code (Ustawa z dnia 6 czerwca 1997…, Art. 270a § 1 and 2 and 277a § 1),
  - issuing or using a false invoice according to the Penal Code (Ustawa z dnia 6 czerwca 1997…,Art. 271a § 1 and 2 and 277a § 1),
- participation in an organised group or association aimed at committing the above-mentioned offences or fiscal offences (Ustawa z dnia 6 czerwca 1997…,Art. 258 § 1-3).

The blocking of the qualified entity's bank account falls:

- at the end of the period specified in the request to block the account for 72 hours or the period for which the blocking was extended for a maximum of three months,
- upon the execution by the bank or SKOK of a request to cancel the blockade issued pursuant to Art. 119zy § 7(2) or Art. 119zw § 5(2) of the Tax Ordinance (Ustawa z dnia 29 sierpnia 1997…),
- when the seizure is made on the basis of:
  - a freezing order issued under the provisions of the administrative enforcement procedure in connection with a notice to block a qualified entity's account for 72 hours to secure a tax or customs debt and interest on arrears,
  - an asset freezing order issued under the provisions of the Code of Criminal Procedure in connection with the notification on blocking the account of a qualified entity for 72 hours

in the part corresponding to the amount specified in the freezing order or asset freezing order, as the case may be.

6.4. Blocking of Bank Accounts in Accordance with Banking Law

Under banking law, account blocking consists of freezing all or part of the funds held in an account. The legal basis for blocking a bank account may be:

- Art. 106 of the Banking Law (Ustawa z dnia 29 sierpnia 1997…),
- Art. 86 of the Anti-Money Laundering and Counteracting the Financing of Terrorism Act (Ustawa z dnia 1 marca 2018…),
- Art. 39 of the Act on Supervision of the Financial Market (Ustawa z dnia 21 lipca 2006…),

According to the Banking Law: "If there is a reasonable suspicion that the bank's activities are being used to conceal criminal activities or for purposes related to a fiscal offence or an offence other than an offence referred to in Article 165a or Article 299 of the Criminal Code – the bank shall notify the public prosecutor, the Police or any other competent authority authorised to conduct preparatory proceedings" (Ustawa z dnia 29 sierpnia 1997…, Art. 106a.1). In such a situation, the bank on its own may take action and block the bank account. The legal basis for the action is Article 106a(3) of the Banking Law: "If a reasonable suspicion arises that the funds accumulated on a bank account, in whole or in part, originate from or are connected with a fiscal offence or an offence other than an offence referred to in Article 165a or Article 299 of the Penal Code, the bank shall be entitled to block the funds on the account. The blocking may only take place up to the amount of funds accumulated in the account suspected of being so" (Ustawa z dnia 29 sierpnia 1997…).

The bank is obliged to notify the law enforcement authorities of suspected criminal use of a bank account, while the blocking of a bank account is optional, not mandatory for the bank. The maximum period of application of an account block by the bank is 72 hours. Immediately after blocking, the bank must notify the public prosecutor who will then decide whether to initiate criminal proceedings within 72 hours calculated from the moment the account is blocked. If proceedings are initiated, the public prosecutor has the option to stop a specific transaction or to block the funds in the account for a specified period of time not exceeding six months from the receipt of the bank's notification of the account blocking.

A person who has experienced a bank account blockage has two types of protection measures aimed at lifting it:

- complaint against an order to apply or extend a blockade,
- request for the blockade to be lifted.

A complaint against the blocking of a bank account must be lodged within seven days from the date of service of the blocking order. The complaint must be lodged with the court having jurisdiction to hear the case, through the public prosecutor who issued the order. It should be noted that despite the filing of the complaint, the blocking of the bank account is maintained and the person is not able to dispose of his/her funds.

Asset freezing can take place on the property of the accused or the suspect. The prosecutor is obliged to formally charge the account holder in the first instance. The law enforcement authorities are more likely to opt for an order based on material evidence as there is no need to charge first (Art. 236b of the Code of Criminal Procedure – Ustawa z dnia 6 czerwca 1997…):

"§ 1. A thing or object within the meaning of the provisions of this Chapter shall also be funds in an account.
§ 2. An order on material evidence may concern funds in an account if they have been retained as evidence in the case".

This interpretation and application of the law has the effect of keeping the bank account blocked for the entire duration of the proceedings, i.e. indefinitely.

Pursuant to Art. 86(1) of the AML/CFT Law, "an obliged institution shall immediately notify the General Inspector, by means of electronic communication, in the event that a reasonable suspicion arises that a specific transaction or specific assets may be related to money laundering or terrorist financing" (Ustawa z dnia 1 marca 2018…).

The General Inspector of Financial Information (GIIF) may

- stop the transaction in question,
- block the bank account for a maximum period of 96 hours.

At the same time, he/she shall notify the competent public prosecutor of the suspected offence of money laundering or terrorist financing. The blocking of the bank account can then be extended by the public prosecutor for a period of six months, or indefinitely if a material evidence order is made.

At the same time, according to Art. 39(1) of the Act on Supervision of the Financial Market: "where it appears from the information obtained which justifies a suspicion that an offence specified in Articles 181-183 of the Act on Trading in Financial Instruments has been committed, that a transaction which has been or is about to be committed may be connected with the commission of that offence, the Chair of the Commission or his/her deputy may apply to the supervised entity with a written request for the blocking carried out by that entity.

(1) a securities account or omnibus account,
(2) another account in which financial instruments that are not securities are recorded,
(3) a cash account
   – for a period not exceeding 96 hours from the time indicated in the request. At the same time as the request, the President of the Commission or his/her deputy shall submit a notification of suspicion of an offence, enclosing information and documents relating to the blocked account" (Ustawa z dnia 21 lipca 2006…).

It therefore follows that the powers of the Chair of the Financial Supervisory Commission are limited to offences against trading in financial instruments, as defined in the special law.

It should also be noted that pursuant to Art. 106a(10) of the Banking Law: "The bank shall not be liable for any damage that may result from the good faith performance of the obligations set out in paragraphs 3 to 5. In such a case, if the circumstances referred to in paragraphs 3 to 5 were not related to the criminal offence or concealment of criminal activities referred to in paragraph 1, the State Treasury shall be liable for the damage resulting from the blocking of funds on the account" (Ustawa z dnia 29 sierpnia 1997…). Such a provision makes it clear that any claim relating to the blocking of a bank account should be addressed to the State Treasury and not to the banks.

The above considerations lead to the conclusion that, first of all, measures should be taken to minimise the risk of the occurrence of events justifying the use of a bank account blockade. This is important in the situation of the crime of money laundering, the statutory prerequisites of which are so broadly defined that, on many occasions, these prerequisites may be fulfilled by entities that do not realise that the funds they receive or trade in may be related to the crime.

A comparison with other forms of account blocking allows a better understanding of the specifics of the procedure applied by the National Revenue Administration. It is also crucial to understand the scope of competence of the Head of KAS and to look carefully at examples of situations in which account blocking may occur. It should be emphasised that it is important to comply with the law and to be cautious in the conduct of one's financial activities when blocking an account.

It is also important to stress that, in accordance with the Supreme Administrative Court resolution, it is possible to remove a taxpayer from the VAT register without notifying the taxpayer (Uchwała NSA z dnia 23 października 2023…). The Court agreed with the tax

authorities that deletion of a taxpayer from the register of active taxpayers under Art. 96(9) (5) of the VAT Act is effected by performing a material and technical act, and therefore also without notifying the taxpayer of this fact (Ustawa z dnia 11 marca 2004…). Note that this resolution is problematic to understand and apply as it concerns the taxpayer's rights and obligations (among others, the right to deduct VAT) and the lack of information on deletion is simply detrimental to the taxpayer. From the taxpayers' point of view, it is therefore reasonable to apply in practice the slogan 'cash is king'. The blocking of accounts (whether under STIR or security or enforcement), is highly problematic and affects both the flow of money and even the perception of the entity by stakeholders. It can bring a business to a standstill, so caution is suggested when dealing with tax authorities.

6.5. Bank Account Blocking in the V4 Countries

In the other V4 countries, namely Czechia, Hungary, and Slovakia the tax administrations have the authority to block bank accounts, though the procedures vary between countries.

- Czechia: the tax administration has the authority to block bank accounts in cases of suspected tax evasion or other tax-related crimes. These procedures are regulated by national tax laws.
- Hungary: the tax authorities can freeze the bank accounts of taxpayers suspected of tax fraud or tax arrears. These procedures are part of measures aimed at ensuring the collection of tax liabilities.
- Slovakia: the tax administration has the authority to block bank accounts in cases of suspected tax evasion or other violations of tax regulations. These procedures are defined in Slovak tax law.

Similarly to Poland, in each of these countries, tax administration procedures for bank account blocking are regulated by local laws and are intended to prevent tax fraud and ensure effective tax collection. When comparing Poland's bank account blocking system to those of the other V4 countries, several key aspects stand out:

- Czechia: the procedures are less automated than in Poland, and their execution depends on specific cases and legal interpretations.
- Hungary: decisions may be based on a narrower range of legal premises, which can affect reaction time and the scope of applied measures. The system is less automated than in Poland.
- Slovakia: the tax administration has the authority to block accounts, but the procedures are more time-consuming and less automated.

6.6. Conclusions

As presented in the chapter, the bank account blockade by the National Revenue Administration is a significant tool intended to secure tax liabilities. Entrepreneurs should be aware of the causes, process, and consequences of such a blockade to appeal effectively against it if necessary, and minimise its negative impact on their businesses.

Administrative courts generally emphasise in their rulings that KAS has the right to block a bank account when a taxpayer has outstanding tax liabilities. However, such actions must comply with applicable legal regulations and general principles, such as proportionality and transparency.

Administrative court rulings play a key role in shaping the practice of applying the regulations on bank account blocking by KAS. Through these rulings, taxpayers can better understand their rights and appeal options. It is worth noting that these rulings may influence future KAS decisions and the way tax authorities approach tax enforcement.

Court judgments highlight the importance of proportionality, transparency, and adherence to procedures, which are crucial for ensuring fairness in the tax enforcement process. These rulings provide taxpayers with an opportunity to effectively assert their rights in cases of unjustified account blockades.

References

Uchwała NSA z dnia 23 października 2023 r., sygn. I FPS 3/23.

Uchwała SN z dnia 26 lutego 2015 r., sygn. III CZP 108/14.

Ustawa z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych (Dz. U. 2025 poz. 163).

Ustawa z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa (Dz. U. 2025 poz. 111).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. Dz. U. 1997 Nr 88 poz. 553 z późn. zm.).

Ustawa z dnia 6 czerwca 1997 r. - Kodeks postępowania karnego (Dz. U. 2025 poz. 46).

Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. 2022 poz. 2324).

Ustawa z dnia 10 września 1999 r. Kodeks karny skarbowy (Dz .U. 2024 poz. 628).

Ustawa z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz. U. 2004 Nr 54 poz. 535 z późn. zm.).

Ustawa z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym (Dz. U. 2022 poz. 660).

Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. 2018 poz. 723 z późn. zm.).

Wyrok NSA z 27 kwietnia 2020 r., sygn. I FSK 491/20.

Wyrok NSA z dnia 26 stycznia 2022 r., sygn. I FSK 2393/21.

Wyrok NSA z dnia 16 lutego 2022 r., sygn. I FSK 2514/21.

Wyrok NSA z dnia 3 czerwca 2022 r., sygn. I FSK 400/22.

Wyrok SN z dnia 3 października 2014 r., sygn. V CSK 630/13.

Wyrok WSA z 10 kwietnia 2020 r., sygn. III SA/Wa 593/20.

Chapter 7

VAT Control Statement

Pavel Semerád

Sting University, Brno
ORCID: 0000-0002-0901-6776

Lucie Semerádová

Ambis University, Prague
ORCID: 0000-0002-1193-7275

Petra Hospodková

Czech Technical University in Prague
ORCID: 0000-0001-6542-8196

Quote as: Semerád, P., Semerádová, L., & Hospodková, P. (2025). VAT Control Statement. In I. Chuy, P. Luty, V. Lakatos (Eds.), *Modern Tools for Fraud Detection: Insights from the V4 and Ukraine* (pp. 85-93). Publishing House of Wroclaw University of Economics and Business.

DOI: 10.15611/2025.40.5.07

7.1. Introduction

Value Added Tax (VAT) fraud can have a long-term negative impact on the market environment. If fraudsters manage to gain a significant market share, they can gradually eliminate honest entrepreneurs, who are then forced to decide whether to adapt to the new market rules and slip into the grey zone themselves, or leave the market. Such a situation is undesirable because it also has a negative impact on public budgets (Dytrychová et al., 2024; Moravec et al., 2021).

In these crisis situations, the state must not hesitate too long to find a solution. If fraud from one sector spreads to others, it can cripple the entire economy – however finding a suitable solution is not easy. Fraudsters are constantly inventing scenarios that allow them to defraud the state of the largest possible amounts of taxes. They use front men who have no idea about their own involvement in the fraud (Knížek, 2013).

After completing the (repeated) fraud, the fraudsters leave behind companies without any liquid assets and completely cut off communication with the tax administrator. This is the scenario used in carousel fraud (Fedeli & Forte, 2011; Olexová et al., 2022). This type of fraud exploits the weaknesses of VAT in intra-Community supplies between at least two European Union countries (see Fig. 7.1).

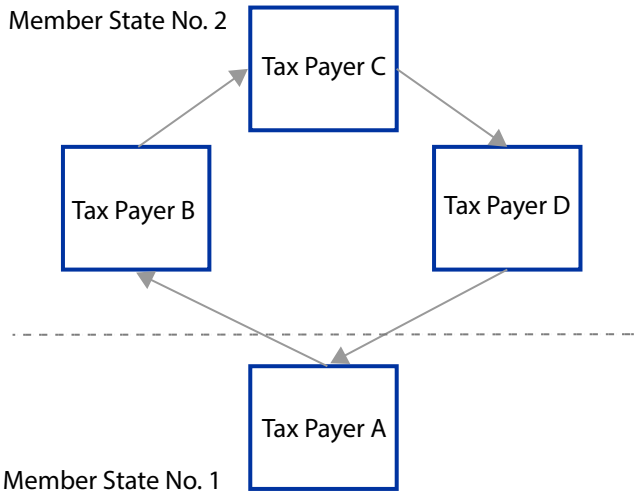


Fig. 7.1. Scheme of carousel fraud

Source: own elaboration.

The carousel fraud begins with Taxpayer A (Member State No. 1) supplying the subject of the transaction to Taxpayer B (Member State No. 2), which is the most risky in terms of the entire tax loss. If, when applying the reverse charge mechanism (Hodinková & Semerád, 2025), it fails to fulfil its tax obligation, Member State No. 2 loses the entire value added tax.

Subsequently, the subject of the taxable supply is delivered to Taxpayer C playing the role of a buffer. Regardless of whether this entity is aware of its involvement in the chain of companies, it performs an important role. It is precisely this entity that enables the tax theft by paying the value added tax to Taxpayer B and subsequently claiming a tax deduction. Thus, the state does not collect any tax and even allows Taxpayer C to claim a deduction.

In the next step, a sale to Taxpayer D may occur, and from there, the goods may return to Taxpayer A in State No. 1, which completes the entire cycle. The result is a tax loss for State No. 2. This procedure can be used several times, and each time, if the fraud is completed, the entire amount of tax is stolen. It is estimated that EU countries lose up to EUR 100 billion each year to carousel fraud (European Commission, 2017).

The only player who directly profits from this fraud is the recipient of the taxable supply. In order to carry out such a large-scale fraud, it is necessary to motivate buyers to purchase the subject of the supply from fraudsters. If business relationships are not based on personal ties, one of the motivational tools is a very low price (unusual price), meaning a price that is not a normal market price or that cannot be obtained without unauthorized tax evasion.

Although with the development of legislation the tax administrator is given a number of effective tools, for example it can apply liability for unpaid tax on transactions at non-market prices (Semerád & Semerádová, 2025), and it is difficult to decipher other entities in the chain. To do this, a digital footprint must be found (most often in the form of a bank transfer payment or a card payment[1]) – using it, it is then possible to decipher which taxpayer paid the fraudster.

[1] Cash payments are problematic. Due to their supervision, countries are introducing electronic sales records, see e.g. (Semerád et al., 2024).

However, fraudsters try to cover their tracks and to hide from the tax administrator, and they also use payments to foreign accounts for this purpose. The tax administrator can usually intervene only when it manages to decipher individual payments. To make the situation even more confusing, fraudulent structures containing several dozen entities from multiple countries can be artificially created. With these groupings, manual control is ineffective and is very time--consuming and personnel-intensive.

An effective aid is the automated processing of data that taxpayers send electronically to the tax administrator in accordance with the value added tax return. The path to digitalisation in cross-border trade is indeed one of the goals of the European Union.

While there are uniform rules for reporting, such as the recapitulative statement, reverse charge and online invoicing for intra-Community supplies, under the VAT in the Digital Age initiative (e.g. IBFD, 2025; Merkx & Gruson, 2025), EU Member States are not unified in the case of domestic supplies. Thus, one may encounter the application of the quick reaction mechanism for various subjects of supply, but its use is time-limited and unsuitable for long--term use.

To be successful in its activities, the tax administrator needs to have real-time data (at the moment of filing the tax return) to be able to carry out cross-checks between taxpayers. This cross-check needs not only be used for carousel fraud, but can equally effectively serve for automated control of reports, for detecting and correcting more or less serious errors and inaccuracies. The errors can be divided into intentional and those caused by incorrect processing.

Intentional errors include:

1. Claiming VAT deductions on fictitious invoices. The taxpayer invents an invoice, and because the tax administrator lacks the tools to verify it, the deduction claim is approved.
2. The same tax document is used by multiple entities. The tax document may be real, but it may be issued for a different taxpayer. Thus, one deduction claim can be applied simultaneously by multiple entities. This occurs in particular with simplified tax documents such as for fuel purchases (Czech Television, 2024), where the recipient of the taxable supply is not specified. The Czech Financial Administration combats this issue by scanning documents during inspections. If repeated use by multiple entities is subsequently detected, their inspection is initiated.
3. The deduction claim is applied to supplies involving an unreliable taxpayer. In such cases, liability for unpaid tax should be applied. However, the tax administrator may not find out in time.

Errors caused by incorrect processing include:

1) The taxpayer claims an incorrect tax rate; usually higher than the one stated on the invoice.
2) The deduction claim is reported in a period with which it is not materially and temporally related (usually earlier than the deduction claim arose). In Czechia, the recipient of the taxable supply can claim a deduction only when the tax document is delivered to them. Thus a sale may take place in January, but if the recipient has the document available only in February, they can claim it no earlier than February.
3) The same tax document can be used twice by one entity. Although accounting software usually alerts the recipient to this error, it can happen that an inattentive accountant applies the same document multiple times.

4) The deduction claim can also be applied when the supply is subject to the reverse charge mechanism, but the accountant forgets to apply the output tax. The recipient makes some other administrative error when transcribing the invoice into the accounting program; this may include an incorrect invoice number (variable symbol).
5) Errors can also occur when transcribing other data. The deduction claim is applied to the supply of goods or services from a non-VAT payer.

To reduce errors in reporting tax liabilities and to protect the good faith of honest entities, it is necessary to use modern elements in tax administration (Semerádová & Semerád, 2022), therefore Czechia introduced the VAT Control Statement in 2016.

7.2. VAT Control Statement

7.2.1. Reasons for Introduction

The tax administrator obtains aggregate information about taxpayers at regular intervals (after the end of the tax period; at most once a quarter). If these taxpayers do not have intra--Community supplies, the tax return is usually the only document from which the amount of input and output tax can be determined. Note that the tax administrator could also use movements on registered bank accounts[2] for ongoing control, and the administrator also had data on cash payments from electronic sales records in the period from 2016 to 2022. Nevertheless, the aggregate information from the tax return is insufficient for the analytical activities of the tax administrator. It is not possible to verify from them whether the aforementioned errors occur when reporting received and issued invoices. This led the Czech tax administrator to seek a tool that would provide more detailed information about individual supplies. This tool became the VAT Control Statement, which, in simple terms, allows control of reported inputs and outputs both on the supplier's side and on the recipient's side of the taxable supply (Table 7.1). Given that the data are cross-referenced even with a time lag (the buyer has several calendar years to claim a deduction), the entire process must work automatically. If the reports contain any discrepancies, for example, invoice numbers, tax bases, or the applied rates do not match, the tax administrator can specifically call on the defaulting taxpayers to correct them.

The VAT control statement was introduced in Czechia on 1 January 2016. It is an electronic form that contains detailed information about all realised and received supplies that a particular taxpayer carried out within the tax period. The individual items are analytically arranged into two parts, A and B. As stated by the General Financial Directorate (2024), including a detailed description of the individual items, and involves:

A. Transactions for which the payer is obliged to declare the tax and supplies in the domestic reverse charge mechanism.

- A.1. Realised taxable supplies in the domestic reverse charge mechanism, for which the recipient of the supply is obliged to declare the tax pursuant.

[2] Taxpayers in Czechia must compulsorily register their domestic bank accounts. These lists are publicly available. If a payment were made to a bank account other than a registered one, the taxpayer would expose themselves to the risk of liability for unpaid tax.

- A.2. Received taxable supplies for which the payer as recipient is obliged to declare the tax pursuant.
- A.3. Realised supplies in the special regime of the investment gold pursuant.
- A.4. Realised taxable supplies and received payments with the obligation to declare tax pursuant in the amount above CZK 10,000, including VAT and all corrections made in connection with irrecoverable claims regardless of the threshold amount.
- A.5. Other realised taxable supplies and received payments with the obligation to declare tax pursuant in the amount up to CZK 10,000, including VAT, or taxable supplies for which the obligation to issue a tax document did not arise.

Table 7.1. Example A of required data in section A.4

No. of line	Tax identification number of customer	No. of tax document	Date of obligation to declare the tax	Tax Base 1	Tax 1	Tax Base 2	Tax 2	Code of VAT regime	Corrections of irrecoverable claims
1	123456789	250123456	02.03.2025	2000	420	–	–	1-§89	–

Source: own elaboration based on the Financial Administration of the Czech Republic (2024).

B. Received taxable supplies with the place of supply in the country.

- B.1. Received taxable supplies in the domestic reverse charge mechanism, for which the recipient is obliged to declare the tax pursuant.
- B.2. Received taxable supplies and provided payments for which the recipient claims VAT deduction pursuant in the amount above CZK 10,000, including VAT and all VAT deduction corrections in connection with irrecoverable claims regardless of the threshold amount.
- B.3. Received taxable supplies and provided payments for which the recipient claims VAT deduction pursuant in the amount up to CZK 10,000, including VAT.

Individual items are clearly and automatically exported from the accounting program. A critical point can be supplies up of to CZK 10,000, where information about the other entity is not provided (Table 7.2). It is naturally less likely that large-scale fraud would be achieved with such small amounts, however the resulting anonymity for certain supplies can arouse distrust.

Table 7.2. Example B of required data in section A.4

Tax Base 1	Tax 1	Tax Base 2	Tax 2	Tax Base 3	Tax 3
5000	1050	–	–	–	–

Source: own elaboration based on the Financial Administration of the Czech Republic (2024).

The amount of CZK 10,000 has a historical connection in Czechia to simplified tax documents, which can only be issued up to that amount, including VAT. A specific feature is that buyer details do not have to be included for these supplies as this obligation arises only on an invoice exceeding this limit.

This information gap was removed in Czechia by electronic sales records which were introduced, among other things, due to fraud in retail, accommodation services, and restaurants (Semerád et al., 2021). By its abolition and the subsequent increase in the limit for VAT registration from CZK 1 million to CZK 2 million, the Czech administration lost valuable data about many entrepreneurs (Semerád et al., 2023), which resulted in the unflattering nickname of 'the dark period'.

7.2.2. Problematic Aspects of the VAT Control Statement

From a technical point of view the VAT control statement was sufficiently prepared. When compared to Slovakia, where the control statement has been in use since 2014 (Financial Administration of the Slovak Republic, 2014; Ministry of Finance of the Slovak Republic, 2020), Slovak taxpayers faced more technical issues when reporting certain taxable transactions (Morávek, 2015).

However, what caused huge concerns on the part of taxpayers were the penalties for errors in submitting the VAT control statement, where penalties ranged from CZK 1,000 to CZK 500,000 depending on the offence[3]. Taxpayers feared that they could be closed down.

Concerns also stemmed from the fact that taxpayers had to respond within five days of the summons, which posed a huge problem, for example, during holidays and when experiencing health problems, compared to Slovakia, where taxpayers have five business days to respond (Mintál, 2024).

Entrepreneurs responded quickly, and the Ministry of Finance of the Czech Republic itself (2016) retroactively amended some legal provisions after ten days of the VAT control statement's effectiveness (Semerád et al., 2016).

A three-month tolerance period was announced, during which penalties were not applied, whereas in Slovakia the first six-month period was exempt from penalties.

Penalties related to the response of taxpayers to the tax administrator's summons, for example, to correct, supplement, or confirm the data contained in the submitted VAT control statement, are subject to the administrative discretion of the tax administrator. The specific amount of the imposed penalty takes into account the significance and potential impact of the breached obligation, as well as the level of cooperation of the taxpayer. Sanctions are also applied in Slovakia, however they are not strictly defined: "The tax office imposes a fine of up to 10,000 euros on the taxpayer. If the taxpayer repeatedly violates the obligations stated in the first sentence, the tax office imposes a fine of up to 100,000 euros. When determining the amount of the fine, the tax office takes into account the severity and duration of the unlawful situation" (Ministry of Finance of the Slovak Republic, 2004…, Section 78a 15).

The established deadline related to the VAT control statement, including the deadline for submitting a subsequent VAT control statement in response to the tax administrator's summons to supplement, change, or confirm data, was adjusted from five calendar days to five working days.

---

[3] If a taxable person registered for VAT does not submit a VAT Control Statement within the due date, the following sanctions will be applied: a) 1000 CZK, if the VAT Control Statement is submitted after the due date without summons from the Tax Administration, b) 10 000 CZK, if the VAT Control Statement is submitted within the deadline given by the Tax Administration in issued and delivered summons, c) 30 000 CZK, if the Corrective VAT Control Statement is not submitted although summons to submit a Corrective VAT Control Statement were issued and delivered by the Tax Administration, d) 50 000 CZK, if the regular VAT Control Statement is not submitted nor submitted after summons of the Tax Administration. Nevertheless, if a taxable person registered for VAT seriously violates or obstructs the administration of VAT by not submitting the VAT Control Statement, the tax administrator can impose a sanction up to 500,000 CZK depending on individual conditions (Semerád & Bartůňková, 2016).

7.2.3. Statistical Review of the VAT Control Statement

The first results of the Financial Administration of the Czech Republic (2016) showed that:

- The Financial Administration received VAT control statements for January 2016 from 245,000 monthly VAT payers (out of 288,000 payers). Most of them submitted the VAT control statement in the correct format.
- Before the commencement of summons to rectify submission defects, most payers corrected their submissions themselves. The original error rate in the submission structure thus decreased from 4% to less than 1%.

The Ministry of Finance of the Czech Republic (2017) subsequently added that after the introduction of the VAT control statement there was a year-on-year increase in VAT revenue of CZK 10-12 billion.

It is clear from these statistics that most VAT payers began to fulfil the obligations arising from the VAT control statement without major technical difficulties immediately from the start of the law's effectiveness. Similarly, the impact on tax revenue, which increased year-on-year, can also be positively evaluated.

Since 2016, the VAT control statement has become a fully automated and trouble-free report that taxpayers send to the tax administrator at regular intervals simultaneously with the tax return. From the perspective of Czechia, one can recommend this measure to tax administrators from other jurisdictions.

7.3. Conclusions

Czechia, like other European Union Member States, has long been fighting value added tax fraud. In the context of intra-Community supplies, standardised tools such as reverse charge, recapitulative statements, VAT in the Digital Age, and other tools after the application of the quick reaction mechanism are used. In the context of domestic administration, however, the solution is the responsibility of individual countries.

It is clear that for effective tax administration it is not enough to have only aggregate information from the tax return, therefore the VAT control statement was introduced in Czechia, providing the tax administrator with detailed information about received and realised taxable supplies.

The data obtained from all taxpayers are subsequently matched, which allows the effective detection of errors in reporting. This can include not only administrative deficiencies (e.g. incorrect invoice number), but also intentional fraud (e.g. reporting fictitious invoices).

The VAT control statement was very well prepared from a technical point of view. Most taxpayers reported their obligations correctly. The error rate was approximately 1%. According to data from the Ministry of Finance of the Czech Republic, there was a year-on-year increase in VAT collection of CZK 10-12 billion.

The only negative point was initially the taxpayers' concerns about high penalties (up to CZK 500,000) and the obligation to respond to the tax administrator's summons within five calendar days. Therefore the Ministry of Finance of the Czech Republic itself retroactively amended some provisions after ten days of the law's effectiveness to prevent the imposition of liquidation fines and to adopt a pro-client approach towards honest taxpayers.

References

Czech Television. (2024). Finanční správa zakročila proti opakovanému vykazování účtenek. https://ct24.ceskatelevize.cz/clanek/ekonomika/financni-sprava-zasahla-proti-opakovanemu-vykazovani-uctenek-354980

Dytrychová, A., Zídková, H., & Arltová, M. (2024). European VAT Collection Under the Stress: Best To Use Few Reduced Rates. *Journal of Policy Modeling*, *46*(6), 1165-1185. https://doi.org/10.1016/j.jpolmod.2024.07.007

European Commission (2017). *European Commission Proposes Far-reaching Reform of the EU VAT System*. https://ec.europa.eu/commission/presscorner/detail/en/ip_17_3443

Fedeli, S., & Forte, F. (2011). International VAT Fraud: The Carousel Game. *Journal of Modern Accounting and Auditing*, *7*(3), 211-226.

Financial Administration of the Czech Republic. (2016). *Kontrolní hlášení: aktuální statistiky z prvního podávání*. https://financnisprava.gov.cz/cs/financni-sprava/media-a-verejnost/tiskove-zpravy-gfr/tiskove-zpravy-2016/kontrolni-hlaseni-aktualni-statistiky-z-prvniho-podavani

Financial Administration of the Czech Republic. (2024). *Guidelines for Filling Out Value Added Tax Listings E-Form (VAT Control Statement)*. https://financnisprava.gov.cz/assets/en/attachments/d-seznam-dani/Control_Statement_Guidelines_20240101.pdf

Financial Administration of the Slovak Republic. (2014). *Kontrolný výkaz*. https://www.financnasprava.sk/sk/podnikatelia/dane/dan-z-pridanej-hodnoty/kontrolny-vykaz-dph

General Financial Directorate (2024). Guidelines for Filling Out Value Added Tax Listings E-Form (VAT Control Statement) version valid since 1.1.2024. https://financnisprava.gov.cz/assets/en/attachments/d-seznam-dani/Control_Statement_Guidelines_20240101.pdf

Hodinková, M., Semerád, P. (2025). VAT Domestic Reverse Charge: Positives and Threats. In I. Chuy, P. Luty, V. Lakatos (Eds.), *Modern Tools for Fraud Detection: Insights from the V4 Countries and Ukraine* (pp. 94-103). Publishing House of Wroclaw University of Economics and Business.

IBFD. (2025). *VAT in the Digital Age (ViDA)*. https://research.ibfd.org/home/content/vat-digital-age-vida

Knížek, J. (2013). Poslanecká sněmovna Parlamentu České republiky. Hospodářský výbor. https://www.psp.cz/sqw/text/orig2.sqw?idd=147931

Merkx, M., & Gruson, J. (2025). EU Member States Agree on ViDA: A Major Step for the EU VAT System and a Digital Leap for Businesses. *EC Tax Review*, *34*(1), 8-21, https://kluwerlawonline.com/journalarticle/EC+Tax+Review/34.1/ECTA2025002

Ministry of Finance of the Czech Republic. (2016). *Andrej Babiš hostem Otázek Václava Moravce*. http://www.mfcr.cz/cs/aktualne/v-mediich/2016/andrej-babis-hostemotazek-vaclava-morav-23633

Ministry of Finance of the Czech Republic. (2017). *Metodika výpočtu dopadů zavedení kontrolního hlášení a elektronické evidence tržeb*. https://www.mfcr.cz/assets/attachments/Informace-zadost-106_Pr-001_2017-05-24_Info-106-99-MF-14863-2017-10-1229IK.pdf

Ministry of Finance of the Slovak Republic. (2004). Act No. 222/2004 Coll. on Value Added Tax. https://www.mfsr.sk/en/taxes-customs-accounting/indirect-taxes/vat/act-222/2004-coll-on-value-added-tax/

Ministry of Finance of the Slovak Republic. (2020). 1 Poučenie na vyplnenie kontrolného výkazu k dani z pridanej hodnoty (ustanoveného opatrením Ministerstva financií SR č. MF/015393/2020-731). https://www.mfsr.sk/files/archiv/92/Poucenie_KV_DPH_2021.pdf

Mintál, J. (2024). *Výzva na podanie kontrolného výkazu a na odstránenie nedostatkov v podanom kontrolnom výkaze*. https://www.dph.sk/33/vyzva-na-podanie-kontrolneho-vykazu-a-na-odstranenie-nedostatkov-v-podanom-kontrolnom-vykaze-uniqueidmRRWSbk196FPkyDafLfWALZKDA4bYb1gNjCOiQ-7f0Y-o0t-Q3epiQ/

Moravec, L., Hinke, J., & Borsiczká, M. (2021). Fiscal Effect of VAT Control Statement – Case Study of the Czech Republic. *Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis*, *69*(3), 365-377. https://doi.org/10.11118/actaun.2021.034

Morávek, D. (2015). *Kontrolní hlášení mají na Slovensku už dva roky. Zjistili jsme, v čem se liší*. https://www.podnikatel.cz/clanky/kontrolni-hlaseni-maji-na-slovensku-uz-dva-roky-zjistili-jsme-v-cem-se-lisi/

Olexová, C., Husťák, M., & Sudzina, F. (2022). Carousel Fraud in Terms of Price Manipulation. *Journal of Financial Crime*, *29*(4), 1329-1340. https://doi.org/10.1108/JFC-07-2021-0169

Semerád, P., Babuněk, O., Brauner, R., Semerádová, L. (2023). Anticipated Effects of the Cancellation of the Electronic Records of Sales System in the Czech Republic. In *Business Environment in a Whirlwind of Turbulent Changes. Proceedings of the 16th International Scientific Conference European Forum of Entrepreneurship 2023* (pp. 252-260). Newton College.

Semerád, P., Bartůňková, L. (2016). VAT Control Statement as a Solution to Tax Evasion in the Czech Republic. *Procedia-Social and Behavioral Sciences*, *220*, 417-423. https://doi.org/10.1016/j.sbspro.2016.05.516

Semerád, P., Radvan, M. Bartůňková, L. (2016). VAT Control Statement Problematic Aspects. In *Proceedings of the 21th International Conference Theoretical and Practical Aspects of Public Finance 2016* (pp. 90-95). University of Economics, Prague.

Semerád, P., Radvan, M., Semerádová, L. (2021). Tax Fraud in Accommodation Services During the COVID-19 Pandemic in the Czech Republic. *Analyses and Studies CASP*, *11*(1), 23-31. https://doi.org/10.33119/ASCASP.2021.1.3

Semerád, P., Semerádová, L. (2025). The Usual Price Rule as a Tool to Detect VAT fraud. In M. Balytska, H. Bohušová, P. Luty (Eds.), *The V4 and Ukraine Fight With Tax Fraud and Money Laundering* (pp. 78-87). Publishing House of Wroclaw University of Economics and Business.

Semerád, P., Semerádová, L., & Dobranschi, M. (2024). Electronic Records of Sales in the Czech Republic. In P. Luty, N. Versal, & P. Semerád (Eds.), *Knowledge and Digitalisation Against Corruption and Fraud* (pp. 78-87). Publishing House of Wroclaw University of Economics and Business.

Semerádová, L., Semerád, P. (2022). Robotics and Automation for Accounting and Tax Purposes. In P. Luty (Ed.), *Fraud in Accounting and Taxation and Its Detection* (pp. 81-94). Publishing House of Wroclaw University of Economics and Business.

Chapter 8

VAT Domestic Reverse Charge: Positives and Threats

Monika Hodinková

Sting University, Brno
ORCID 0009-0007-5852-3399

Pavel Semerád

Sting University, Brno
ORCID 0000-0002-0901-6776

Quote as: Hodinková, M., & Semerád, P. (2025). VAT Domestic Reverse Charge: Positives and Threats. In I. Chuy, P. Luty, V. Lakatos (Eds.), *Modern Tools for Fraud Detection: Insights from the V4 and Ukraine* (pp. 94-103). Publishing House of Wroclaw University of Economics and Business.

DOI: 10.15611/2025.40.5.08

8.1. Introduction

Value Added Tax (further VAT) is an indirect tax that represents a significant source of revenue for public budgets within the Member States of the European Union. One of its main advantages is that it facilitates cross-border trade and supports the EU single market (Keen & Lockwood, 2010).

Despite its robust structure, VAT is often subject to various forms of tax fraud, which have serious implications for economic stability and fair competition. Among the most significant and complex scams are the so-called carousel frauds (European Commission, 2021). These frauds include the (repeated) resale of goods between related entities in different Member States of the European Union, where one of the links in the chain (the so-called missing trader) does not pay VAT and subsequently becomes non-contactable (Arltová et al., 2020).

In this way, tax benefits are unjustifiably obtained and public budget revenues are significantly lost. According to the European Parliament (2021), annual losses due to carousel fraud amounted to EUR 60 billion, underlining the seriousness of the problem.

Although these types of fraud are well known, eliminating them is quite challenging. Considering that fraud is (often) organised by multinational groups using multiple actors in the chain, the overall effectiveness is further hampered by the different tax rules operating across the Member States of the European Union. For example, in the Admiral 2.0 case, 400 entities from 15 European Union Member States were involved in fraud (European Public Prosecutor's Office, 2024).

The principle of carousel fraud is presented in more detail in Fig. 8.1. Taxpayer A sells goods to Taxpayer B. In this case, it is a standard supply of goods to another Member State of the EU, which is exempt from tax with the right to deduct. At the same time, Taxpayer A duly claims a VAT deduction if he meets the legislative requirements in his country. Taxpayer B is obliged to apply the reverse charge. This means that the output tax on the purchased goods is declared, while at the same time (if the statutory conditions are met) the right to deduct VAT is applied.

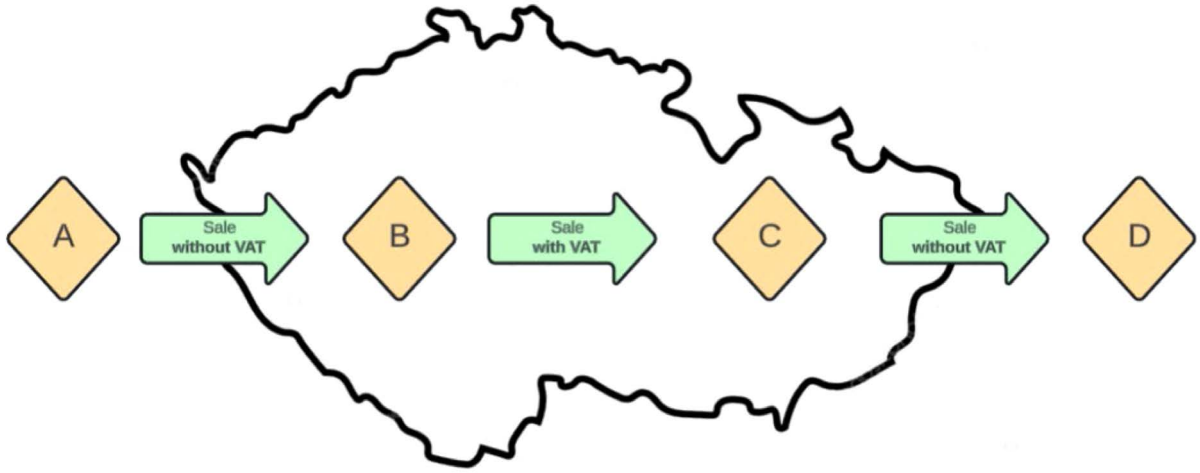


Fig. 8.1. The principle of carousel fraud

Source: own elaboration based on (European Parliament, 2021).

Next, Taxpayer B sells the goods to Taxpayer C in the same country, adding VAT at the statutory rate to its selling price as a taxpayer. Taxpayer B receives the total payment including VAT from Taxpayer C, but without paying it. The tax return is either not filed in properly or it is claimed that there are not enough liquid resources to pay the tax.

This step is a crucial part of the fraud that damages the principles of VAT in the given jurisdiction. The tax administrator relies on the honesty of the taxpayer to meet the obligation to pay output tax and at the same time to claim input tax. Although there is zero tax liability from this transaction, for a sale to Taxpayer C, the seller is obliged to pay output VAT. However, this is no longer the case because immediately after receiving VAT on this transaction from the buyer, the so-called missing trader concludes the business without any liquid assets (Semerád & Semerádová, 2025).

Finally, Taxpayer C can continue to trade in the goods and, for example, sell them to Taxpayer D in another Member State of the EU. This is again considered to be a supply of goods to another EU Member State, i.e. one exempt from tax with the right to deduct tax, which Taxpayer C can claim in its jurisdiction. If the tax administrator fails to prove that Taxpayer C "knew or should have known" about the fraudulent conduct, and the tax fraud is complete.

In addition to carousel fraud, value added tax fraud also includes fictitious invoicing, falsification of tax documents, and abuse of the VAT refund system.

Fictitious invoicing consists of issuing tax documents for non-existent supplies with the aim of unduly reducing the tax liability for the VAT payment or obtaining an excessive deduction[1]. For

[1] Excess deduction means tax corresponding to the difference between the output tax and the tax deduction for the tax period if the output tax is lower than the tax deduction.

example, the Customs Administration of the Czech Republic (2023) uncovered a group of legal entities that had unjustifiably reduced VAT payments by at least CZK 12 million through fictitious invoices for unperformed work and supplies of materials in the field of wood processing.

Falsification of tax documents involves altering real documents or creating completely false documents in order to evade tax or obtain unjustified tax advantages. In practice, this includes handling accounting documents or failure to post issued invoices.

The danger of this fraud lies in the fact that it can be combined, nevertheless the reverse charge mechanism is an essential part of value added tax. Its popularity is also growing in domestic supplies as it eliminates the possibility of an unjustified VAT deduction claim by the customer. This has proven to be an effective means of combating tax fraud, especially in high--risk sectors such as construction, trade in electronics, emission allowances and agricultural products[2]. Czechia managed to minimise tax evasion and increase the transparency of business transactions conducted there.

However, the financial administration is not always successful in marketing this tool to the public, even though, according to Grásgruber et al. (2013) and the Chamber of Tax Advisors of the Czech Republic (2021), its implementation brings positive results, including the prevention of tax fraud:

- entrepreneurs complain about the increased **administrative burden** as they have to monitor their business transactions more closely and ensure that the reverse charge regime is applied correctly;
- new forms of fraud **are emerging** that circumvent existing control mechanisms (e.g. issuing fake VAT payers who abuse the reverse charge mechanism to obtain goods without value added tax).

It is therefore necessary for the financial administration to continuously monitor the effectiveness of reverse charge, and if problems are identified, to adjust the legislative framework. The aim is to reflect current developments and eliminate new threats in the field of tax fraud.

In this chapter, the authors focused on the domestic reverse charge mechanism, as its parameters can be largely determined by the EU Member State. However, it may be limited by other EU Member States, as happened in Czechia e.g. in the case of fuel trading (Semerád, 2014).

The EU can also apply temporary solutions through the Quick Response Mechanism (further QRM), a tool that allows for responding quickly and effectively to sudden and large-scale tax fraud in a specific area of value added tax. This mechanism enables, for example, the introduction of a reverse charge regime in areas with an identified high risk of fraud.

In Czechia the rapid response mechanism is implemented through Section 92g of Act No. 235/2004 Coll., on Value Added Tax. This mechanism allows the government, based on the approval of the European Commission, to temporarily introduce a reverse charge regime for a selected type of specific goods or for the provision of a specific service for which a high risk of tax evasion has been identified. The measure was implemented in practice through

[2] According to the Financial Administration of the Czech Republic (2016), fraud was detected on the meat market, where tax evasion amounted to up to CZK 1 billion. These types of fraud concerned not only Czechia, but all the members of the Visegrad Four had to deal with them.

Government Decree No. 361/2014 Coll., and managed to reduce the number of fraudulent transactions and increase the efficiency of VAT collection in the given areas.

However, it is also important to note that the use of the rapid reaction mechanism is limited in time. This restriction ensures that measures are applied only when necessary and for the time necessary to suppress the identified fraud. After the expiry of the specified period, the situation must be re-evaluated and a decision must be made on the possible extension or termination of the measure. The rapid reaction mechanism is possible under Section 92g(1) of the Art. 2 of the VAT Act can only be applied for a period not exceeding nine months, moreover the European Commission must also agree to its use (see Section 92g(1) of the VAT Act).

8.2. Domestic Reverse Charge Mechanism in the V4 Countries

According to Stanley-Smith (2017), the countries in Central Europe are the most affected by VAT fraud. The introduction of the reverse charge mechanism has therefore become an important step towards tackling VAT fraud and increasing the efficiency of VAT collection in the V4 countries (Bogdanski, 2015; Kútna et al., 2018). An overview of how the reverse charge regime is implemented in the V4 countries is given in Table 8.1.

Table 8.1. General and national EU reverse charge rule by country

Country	General reverse charge (Art. 194)	National reverse charge (Art. 199)						
	Domestic goods	Real estate	Installation	Construction	Metal	Mobile phones	Gas and electricity	Carbon trading
Czechia	yes	–	yes	yes	yes	yes	yes	yes
Hungary	–	yes	yes	yes	yes	–	yes	yes
Poland	yes	–	yes	yes	–	–	yes	yes
Slovakia	yes	yes	yes	yes	yes	yes	yes	yes

Source: own elaboration based on (Caragher, 2024).

8.2.1. Domestic Reverse Charge Mechanism in Slovakia

The reverse charge mechanism in Slovakia entered into force in January 2016 and its application was focused on construction works. According to Kútna et al. (2018), the aim of introducing the reverse charge mechanism was to improve the business environment. However, two years of experience with the reverse charge mechanism in the Slovak construction sector revealed negative impacts, especially on the cash flow of construction companies.

8.2.2. Domestic Reverse Charge Mechanism in Poland

Spychalski (2014) stated that the Polish national reverse charge mechanism was applied to mobile phones, laptops and game consoles. Since 2015 the reverse charge mechanism has also been applied to gold ore and certain steel products whose characteristics are similar to those already covered by the reverse charge mechanism.

An important point is that these goods are subject to the reverse charge mechanism only if the total net value of the goods in the so-called economically unitary transaction exceeds PLN 20,000 (USD 5,000). Bogdanski (2015) also noted that another measure to prevent tax fraud is the reporting obligation. The authorities have introduced a new type of tax return, called Recapitulative Statement in Domestic Transactions, where VAT payers who carry out supplies subject to the local reverse charge regime are obliged to submit this report.

According to Fornalik (2017) and Martko-Mazur and Sagan (2018), new rules under the reverse charge mechanism were also introduced for domestic supplies ofconstruction works between two VAT payers (only for construction works defined in Annex 14 to the VAT Act). There is an objective condition that requires that the service provider is not exempt from VAT, that the recipient of the service is registered as an active VAT payer and, last but not least, that the service provider acts as a subcontractor.

8.2.3. Domestic Reverse Charge Mechanism in Hungary

According to MAROSA (2023), from 1st January 2024, Hungarian subcontractors have greater responsibility for services in the construction industry, with a shift from the main contractor to the subcontractor (service provider). The transition to the new reverse charge mechanism requirements requires a proactive approach on the part of companies operating in the field of construction and assembly services in Hungary. Adapting to the updated reverse charge mechanism is crucial for compliance and credibility in the construction sector. The main change is the condition that the construction activity must be subject to an official authorisation or notification to the competent authority in order for the reverse charge mechanism to apply. The scope of activities that fall under the reverse charge mechanism for construction services includes activities of construction, installation and other miscellaneous assembly work aimed at the construction, extension, conversion or other modification of real estate.

Caragher (2024) further stated that Hungary is the last country to introduce a reverse charge mechanism for domestic gas trading transactions. This step reduced potential fraud in transactions between wholesale companies.

8.2.4. Domestic Reverse Charge Mechanism in Czechia

The reverse charge mechanism transfers the obligation to declare and pay value added tax from the supplier to the customer. This system is designed to minimise tax fraud by shifting the tax liability to the recipient of the taxable supply, which means that the recipient of this taxable supply is the person who is obliged to declare the tax on the date of the taxable supply in Czechia.

In general, domestic reverse charge can be characterised as the principle of transferring tax liability from the supplier to the person who purchases goods or uses services. In the case of domestic reverse charge, VAT is paid by the customer of the goods or the recipient of the service. In Czechia domestic reverse charge concerns, among others, purchases of gold, construction and assembly work, supplies of mobile phones, provision of telecommunication services, or the sale of game consoles, tablets or laptops, etc. According to the current VAT Act in Czechia, the reverse charge may be permanent or temporary (Otavová & Grásgruber, 2015).

The permanent application of the reverse charge mechanism applies to specific supplies and services, such as the supply of gold (Section 92b of the VAT Act), the supply of real estate (Section 92d of the VAT Act), the provision of construction or assembly work (Section 92e of the VAT Act), or the supply of goods listed in Annex No. 5 to the VAT Act (Section 92c of the VAT Act).

The temporary application of the reverse charge mechanism is then used in practice on the basis of an approved government regulation. This regime applies to goods or services listed in Annex No. 6 to the VAT Act, such as the supply of mobile phones, the supply of equipment with integrated circuits or the transfer of greenhouse gas emission allowances, etc.

8.3. Advantages of Using the Domestic Reverse Charge Mechanism

The reverse charge mechanism in the area of value added tax brings advantages that contribute to more efficient tax collection and reduction of tax evasion (Ministry of Finance of the Czech Republic, 2015). Examples include resistance to tax fraud and registration requirements.

Resistance to tax fraud. EY (2024), Stiller and Heinemann (2024), Butu et al. (2020) and Buettner and Tassi (2023) agree that reverse charge mechanism is one of the most important measures to combat VAT fraud, achieved by shifting the VAT obligation from the supplier to the customer in business-to-business transactions. However, there is a risk that fraud may shift from countries applying the reverse charge mechanism to countries that do not yet fully use the reverse charge mechanism. This phenomenon clearly highlights the need for a unified approach to EU-wide VAT fraud.

Registration REQUIREMENTS

VAT payers must document their transactions and thoroughly verify their business partners. This procedure increases the transparency of business relations and reduces the risk of business entities engaging in fraudulent activities. For example, in the construction industry in Czechia, the reverse charge mechanism is applied to the provision of construction or assembly work, which requires very careful records and a thorough verification of their business partners from the persons involved, which significantly increases transparency in this sector.

It follows from the above that the implementation of the reverse charge mechanism brings significant benefits in the fight against tax fraud, increases the transparency of commercial transactions and contributes to more efficient tax collection overall.

Extending the use of the reverse charge mechanism in Czechia would lead to a further reduction in the number of cases of VAT fraud, but so far this extension has not been incorporated into national legislation. The reason may also be the fact that the ongoing financing of the public budget would be disrupted. Value added tax is paid on a monthly or quarterly basis, while in the reverse charge mechanism, there is no ongoing payment of VAT on a specific supply.

8.4. Risks Associated with the Use of Reverse Charge

As experience from Czechia shows, the use of reverse charge may also be associated with risks that expose honest VAT payers to the risk of becoming guarantors for unpaid tax.

There are known examples of orders from fictitious VAT payers and the subsequent delivery of goods that were under the reverse charge mechanism. As Hraba (2015) stated, fraudsters abused this in the case of electronics, where local reverse charge was applied, however this could only occur between VAT payers. Fraudsters ordered goods as fictitious VAT payers and e-shops incorrectly invoiced these goods in the reverse charge mode. As a result, e-shops had to pay VAT to the state, even though they had not received it paid by fraudsters. In cases of repeated fraud, this could result in liquidation of e-shops due to their low margins.

8.5. Proposal to Reduce Administration and Risk

The reverse charge increases the administrative demands on the payers because they have to distinguish which supplies are to be applied. Some transactions may be difficult to define and can be interpreted in two ways. Any uncertainty on the part of payers is problematic, because they can then make an unintentional mistake due to ignorance.

For this reason, the reporting rules are shifting. Judging from experience in Czechia, it is **difficult to identify such supplies in construction and assembly work**. Therefore, the legislator allows for the option that if taxpayers agree among themselves on the application of the reverse charge tax liability, they may do so even in cases of a supply that would otherwise be without the reverse charge. This increases the legal certainty of payers who do not make a mistake. The reverse charge must be viewed as a tool that prevents tax fraud as taxpayers should not be punished if they apply it in good faith.

The administration may benefit from **setting a limit** from which the reverse charge mechanism will be applied (e.g. regarding delivery of goods). For less significant items, it might be easier to apply a standard calculation containing value added tax. For transactions of a higher value or risky commodities, a limit may be set from which the reverse charge is mandatorily required – in Czechia this limit was set at CZK 100,000 (Sobotková, 2015).

8.6. Conclusions

Domestic reverse charge is an effective tool in the fight against tax fraud in risky commodities. Its implementation in the national legislation of the European Union Member States contributes to strengthening the fiscal integrity and transparency of the tax system, as shown by the example of Czechia Republic. However, for this mechanism to be truly effective it is necessary to take additional measures.

These measures include caution on the part of payers and consistent control of business partners. VAT payers must carefully verify the reliability of their suppliers and customers in their own interest in order to avoid involvement in fraudulent schemes. This prevention includes checking the VAT registration, financial stability and business history of the partners. Implementing internal controls and rules can significantly reduce the risk of inadvertent involvement in tax fraud. This is also required by the judgments of the European Court of Justice and domestic courts[3] working with the assumption that the payer knew or should have

[3] The judgments in Joined Cases C-354/03, C-355/03 and C-484/03 Axel Kittel v Belgium and Axel Kittel v Belgium (C-439/04) and in the Joined Case Belgian State Treasury v Recolta Recycling SPRL (C-440/04) of 2006 are groundbreaking (Court of Justice of the European Union, 2006a, 2006b).

known that he (or she) was part of a fraudulent structure. This is related to the subsequent possibility of applying a guarantee for unpaid tax in Czechia (Semerád & Semerádová, 2025).

Although this provision can be viewed as a hard tool in tax administration, it is primarily necessary to use the principle of taxes as a contribution to the running of public affairs and it is therefore necessary to defend the interests of the state (Boháč, 2018). Without the active participation of VAT payers in the prevention of tax fraud, it would be very difficult to effectively combat sophisticated fraudulent schemes such as carousel fraud.

To combat tax fraud, domestic reverse charge can be used, applied especially in the taxation of intra-community supplies. As shown by the results from Czechia, the benefit of this measure is greater resistance to tax fraud in risky commodities, yet there are known cases where this legislation was abused by fraudsters against careless taxpayers who did not verify whether the client was really a VAT payer. Fraudsters pretended to be taxpayers, thus obtaining goods without value added tax, and sellers then had to pay value added tax, even though they did not collect it from customers. Despite this negative impact, the domestic reverse charge can be seen as an effective measure.

References

Act No. 235/2004 Coll., on Value Added Tax, as amended. https://www.zakonyprolidi.cz/translation/cs/2004-235?langid=1033

Arltová, M, Pavel, J., Tepperová, J., & Zídková, H. (2020). What Are Effective Measures Against VAT Evasion? Evidence from the Czech Republic. *Ekonomický časopis (Journal of Economics)*, *68*(2), 147-167.

Bogdanski, B. (2015). Poland: Amendments to the Polish VAT Act. *International Tax Review*. July 2015. https://www.internationaltaxreview.com/article/2a68rfy5bw2ycq0s5ra08/poland-changes-to-the-polish-vat-law

Boháč, R. (2018). Registration of Sales in the Czech Republic with Regard to the Decision of the Constitutional Court. In J. Andraško, J. Hamuľák, M. Kahounová (Eds.), *Bratislava Legal Forum 2018*. https://www.flaw.uniba.sk/fileadmin/praf/Veda/Konferencie_a_podujatia/bpf_2018_new/Zbornik_BPF2018_sekcia_2

Buettner, T., & Tassi, A. (2023). VAT Fraud and Reverse Charge: Empirical Evidence from VAT Return Data. *International Tax and Public Finance*, *30*(1), 849–878. https://doi.org/10.1007/s10797-023-09776-y

Butu, I., Brezeanu, P., & Ghetu, R.-A. (2020). Reverse Charge and VAT Gap – A Mechanism to Tackle Intra--Community VAT Fraud. In C. Bratianu, A. Zbuchea, F. Anghel, B. Hrib (Eds.). *Strategica: Preparing for Tomorrow, Today. International Academic Conference – Eighth Edition – Bucharest, October 15-16, 2020* (pp. 396-410). https://strategica-conference.ro/wp-content/uploads/2022/04/29-1.pdf

Caragher, J. (2024). *Hungary 2025 Fight Against VAT Fraud in Connection with Gas in the Czech Republic Reverse Charge*. https://www.vatcalc.com/hungary/hungary-2025-anti-vat-fraud-gas-domestic-reverse-charge/

Chamber of Tax Advisors of the Czech Republic. (2021). *Reverse Charge: An Effective Tool Against Fraud? The Czech Republic Has Not Managed to Introduce It Across the Board.* https://www.kdpcr.cz/pronbspmedia/temata-a-komentare/reverse-charge-ucinny-nastroj-proti-podvodum-cesko-jej-plosne-zavest-nestihlo

Court of Justice of the European Union. (2006a). *Judgment of the Court (Second Chamber) of 12 January 2006 in Joined Cases C-354/03, C-355/03 and C-484/03, Optigen Ltd, Fulcrum Electronics Ltd and Bond House Systems Ltd v Commissioners of Customs & Excise.* https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A62003CJ0354

Court of Justice of the European Union. (2006b). *Judgment of the Court (Grand Chamber) of 6 July 2006 in Cases C-439/04 and C-440/04, Axel Kittel v Belgium and Treasury of Belgium v Recolta Recycling SPRL.* https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A62004CJ0439

Customs Administration of the Czech Republic. (2023). *Fraud with Fictitious Invoices Contributed to a Profit of at Least 12 Million Crowns.* https://celnisprava.gov.cz/cz/tiskove-zpravy/2023/Stranky/Podvody-s-fiktivn%C3%ADmi-fakturami-p%C5%99isp%C4%9Bly-k-zisku-minim%C3%A1ln%C4%9B-12-milion%C5%AF-korun.aspx?utm_source=chatgpt.com

European Commission. (2021). *VAT Carousel Fraud*. https://taxation-customs.ec.europa.eu/taxation/vat/fight-against-vat-fraud/vat-carousel-fraud_en

European Commission. (2025). *VAT Special Schemes*. https://taxation-customs.ec.europa.eu/taxation/vat/vat-special-schemes-oss_en

European Parliament. (2021). *Missing Trader Intra-Community Fraud.* https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690462/IPOL_BRI(2021)690462_EN.pdf

European Public Prosecutor's Office. (2024). *Investigation Admiral 2.0: Europe's Biggest VAT Fraud with Links to Organised Crime.* https://www.eppo.europa.eu/en/media/news/investigation-admiral-20-europes-biggest-vat-fraud-links-to-organised-crime

EY. (2024). *Worldwide VAT Guide for 2024*. https://www.ey.com/cs_cz/technical/tax/tax-alerts/2024/03/ey-celosvetovy-pruvodce-dph-pro-rok-2024

Financial Administration of the Czech Republic. (2016). *Warning About VAT Fraud in the Meat Market.* https://financnisprava.gov.cz/cs/financni-sprava/media-a-verejnost/tiskove-zpravy-gfr/tiskove-zpravy-2016/upozorneni-na-podvody-s-dph-na-trhu-s-masem

Fornalik, J. (2017). Poland: Reverse Charge of National Construction Services. *International Tax Review.* March 2017. https://www.internationaltaxreview.com/article/2a68raha94goaj1osmrdc/poland-reverse-charge-on-domestic-construction-services

Government Decree No. 361/2014 Coll., on the Determination of the Supply of Goods or Provision of Services for the Application of the Reverse Charge Regime of 22 December 2014.

Grásgruber, M., Otavová, M., & Semerád, P. (2013). Impacts of the Application of the Reverse Charge Mechanism of the Value Added Tax. *Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis*, *61*(7), 2133-2141. https://doi.org/10.11118/actaun201361072133

Hraba, L. (2015). *E-Shops, Beware of VAT Fraud!* https://zpravy.kurzy.cz/383920-e-shopy-pozor-na-podvody-s-dph/

Keen, M., & Lockwood, B. (2010). The Value Added Tax: Its Causes and Consequences. *Journal of Development Economics*, *92*(2), 138-151. https://doi.org/10.1016/j.jdeveco.2009.01.012

Kútna, A., Gyurián, N., & Šeben, Z. (2018). Impact of the Reverse Charge Mechanism in the Area of VAT on the Cash Flows of Construction Companies in the Slovak Republic. In P. Hajek, O. Vit (Eds.), *Innovations in Science and Education: CBU International Conference Proceedings March 2018, 21-23, Prague.* CBU Research Institute.

MAROSA. (2023). *Changes to the Hungarian Reverse Charge in the Construction Sector*. https://marosavat.com/changes-in-the-hungarian-reverse-charge-construction/

Martko-Mazur, K., & Sagan, M. (2018). Mechanism of Reverse Charge to Value Added Tax in Transactions Related to the Provision of Construction Services – Selected Issues. In M. Sentsova (Karaseva), E. Ruskowski, A. Paul, M. Radvan (Eds.), *Tax Sovereignty and the Concept of FISCAL RULE-MAKING in Central and Eastern European Countries* (pp. 296-306). Voronezh State University Publishing House.

Ministry of Finance of The Czech Republic. (2015). *Proceedings of the Reverse Charge Conference*. https://www.mfcr.cz/assets/attachments/Material_2015-12-04_Sbornik-ke-konferenci-o-reverse-charge.pdf

Otavová, M., & Grásgruber, M. (2015). *Impacts of the Application of the Reverse Charge Regime for Value Added Tax*. https://www.dauc.cz/clanky/5312/dopady-uplatnovani-rezimu-preneseni-danove-povinnosti-u-dane-z-pridane-hodnoty

Semerád, P. (2014). *Fraud on General Excise Duty on Fuel*. Mendel University. Doctoral thesis.

Semerád, P., & Semerádová, L. (2025). The Usual Price Rule as a Tool to Detect a VAT Fraud. In M. Balytska, H. Bohušová, P. Luty (Eds.), *The V4 and Ukraine Fight with Tax Fraud and Money Laundering* (pp. 78-87). Publishing House of Wroclaw University of Economics and Business.

Spychalski, M. (2014). Poland: Draft Amendment to the VAT Act to Combat Tax Fraud. *International Tax Review*. October 2014.

Stanley-Smith, J. (2017). EU to Choose the 'Nuclear Option' on VAT Fraud in Reverse Charge Systems. *International Tax Review*. https://www.internationaltaxreview.com/article/2a68raha94goaj1oslcvk/eu-to-take-nuclear-option-on-vat-fraud-with-reverse-charge-systems

Stiller, W., & Heinemann, M. (2024). Do More Harm Than Good? The Optional Reverse Charge Mechanism against Cross-Border Tax Fraud. *Quarterly Review of Economics and Finance*, *95*, 61-84. https://doi.org/10.1016/j.qref.2024.02.007

Chapter 9

Non-Financial Reporting Versus Corruption and Bribery – Practice of Polish Listed Companies

Katarzyna Piotrowska

Wroclaw University of Economics and Business
ORCID: 0000-0002-5830-6526

Quote as: Piotrowska, K. (2025). Non-Financial Reporting Versus Corruption and Bribery – Practice of Polish Listed Companies. In I. Chuy, P. Luty, V. Lakatos (Eds.), *Modern Tools for Fraud Detection: Insights from the V4 and Ukraine* (pp. 104-119). Publishing House of Wroclaw University of Economics and Business.

DOI: 10.15611/2025.40.5.09

9.1. Introduction

When conducting business, companies are required to report both on the state of their assets and the effects of their operations in publishing mandatory financial statements. In addition, they disclose non-financial information, most often in the form of a report on non-financial information because this is an important part of business entities' communication with the public. The scope and type of non-financial information disclosed is governed by balance sheet law. The growing interest in ethical issues, transparency and sustainability in the business environment also affects the growth of information needs in the field of anti-corruption, as corruption negatively affects economic development and public confidence. Security issues in the field of anti-corruption are important for the smooth running of business, which is why also in Poland business entities are obliged to report information on their activities in this regard. This is done specifically within the framework of non-financial reporting.

The purpose of the study was to diagnose the situation of companies in terms of reporting anti-corruption information as part of non-financial reporting. The subjects were Polish listed companies (WIG40), and the Orlen Group and Orlen SA were selected for the first stage. The author examined the information on anti-corruption and bribery revealed in the reports on non-financial information in the period 2017-2023 for the selected entities, including a case study for one of these entities. The following research methods were used to achieve the research objective: qualitative analysis, synthesis, deduction and induction, comparative analysis, and inference by analogy of phenomena.

The research process consisted of a preliminary study (the case study covered by this paper, preparation of proposals for areas to be evaluated for the preparation of a research tool, i.e. assessment questionnaire) and the study proper (the validation of the research tool on

a selected subject, diagnosis of the practice of Polish listed companies in the studied scope based on content analysis of non-financial reports).

The rationale for addressing this issue was the research gap due to the paucity of academic publications linking non-financial reporting issues to anti-corruption and bribery information (the result of a search in the Scopus database, according to the string: TITLE-ABS-KEY 'non--financial reporting' and 'anti-corruption', was found in ten publications). The nature of the study is cognitive (diagnosis of the reporting practice of listed companies) and applied (filling the information gap through the implementation of good practices of non-financial reporting in the field of anti-corruption).

9.2. Literature and Regulatory Review

Many publications on non-financial reporting issues can be identified in the literature (Baboukardos et al., 2023; Bąk et al., 2022; Bek-Gaik & Surowiec, 2020; Błażyńska, 2018; Krasodomska et al., 2018; Matuszak & Różańska, 2021; Mysaka & Derun, 2024; Turzo et al., 2022; Yadav et al., 2024). Corruption issues, due to the nature of the problem, were also addressed, however there is a lack of research combining both areas. Analysis of the scope, type and manner of reporting of the effects of companies' anti-corruption and bribery activities is not often conducted. Note that in Poland legislative changes in the field of non-financial reporting also require some reflection. This indicates the type of research gap and the legitimacy of taking up this topic.

As already highlighted, the sheer scope of research on non-financial reporting is extremely broad, including literature reviews. Turzo et al. (2022) aimed to summarise the various research on non-financial reporting (NFR) practices and the evolution of NFR research by providing a review based on the most influential articles published between 2012 and 2020. They used bibliometric analysis to identify eight research areas: the content of non-financial reports, the integrated reporting (IR) framework, the relation of NFR with company-level variables, and between NFR and corporate governance, the theories behind NFR, NFR assurance, the relation between institutional context and NFR, and also environmental reporting (Turzo et al., 2022). In turn, the study by Mysaka and Derun (2024) was the first to compare the bibliometric characteristics of SR and NFR publications to determine the use of SR and NFR theoretical frameworks for implementing CR in the form of EU directives.

In Poland, research has been undertaken extensively in the years of implementation of EU Directive 2014/95/EU and national regulations as a result of the transposition (European Union, 2014). With the introduction of the regulations, certain groups of entities were required to disclose non-financial information on environmental, social and labour issues, respect for human rights, anti-corruption and anti-bribery activity. Hence, Matuszak & Różańska (2017) analysed the scope and quality of Corporate Social Responsibility (CSR) reporting on companies listed on the Warsaw Stock Exchange (WSE) and their compliance with the new requirements, using a sample of 150 selected listed companies. At the time, according to the study, companies placed little emphasis on human rights and anti-corruption reporting. Their research continued in subsequent years with a sample of 134 selected companies, using content analysis and a disclosure index applied to measure the level of non-financial disclosure (NFD). The study compared non-financial reporting practices in the two years before (2015) and one year after (2017) the implementation of the directive. The results indicated that there was already a high level of compliance with European Union regulations. The coverage of the NFD in various

thematic aspects in the reporting media increased significantly between 2015 and 2017, particularly in the areas of human rights and anti-corruption. The research suggested that stakeholders should receive the more comprehensive information they need in their decision--making process (Matuszak & Różańska, 2017).

As the literature review showed, the experience of other countries is similar. Carmo and Ribeiro (2022) conducted an analysis of the content of non-financial disclosures made one year before (2016) and in the first and second year of implementation of Directive 95/2014/EU (2017 and 2018) in their country. The results showed that the greatest impact on the quality of non-financial disclosures was observed in the first year of the directive. Companies that had high quality voluntary reporting practices, such as a presentation of a sustainability report, the use of GRI standards and NFI certification (Mbanyele et al., 2022), maintained these practices after the introduction of the directive. However, there were still companies that did not mention the framework used or did not disclose information on sensitive issues such as human rights, anti-corruption and anti-bribery (Carmo & Ribeiro, 2022).

Non-financial reporting, strictly in the context of anti-corruption, has been analysed to a lesser extent. Aldaz et al. (2015) investigated whether companies' anti-corruption reporting practices reflected the respective anti-corruption systems implemented by the companies, or whether disclosure was merely a tool for these companies to improve their reputation and thus maintain their legitimacy, using both legitimacy theory and stakeholder theory (Aldaz et al., 2015). This still seems to be the case in the context of the division between values-driven CRS reporting or submissiveness-driven CSR (Roberts et al., 2008). Landis and Paglietti (2024) examined corporate anti-corruption disclosure (ACD) strategies during the regulatory debate surrounding European Directive 2014/95/EU. Using a legitimacy framework, they assessed whether companies proactively improved their voluntary ACDs during the transposition phase to accommodate potential regulatory changes (Landis & Paglietti, 2024).

In today's Poland, research in this area is also being published. Aluchna et al. (2024) examined the relation between company links with the external environment, proxied by board independence and ownership dispersion, and anti-corruption disclosure. The authors used a sample of 72 companies listed on the Warsaw Stock Exchange over the period of 2015-2019 that were subject to the NFRD legislation. The evidence from the Tobit model showed that the links with the external environment differentiated company reactions to the implementation of the mandatory reporting legislation. In particular, extensive company links via interdependent directors and ownership dispersion increase the scope of the anti-corruption (Aluchna et al., 2024). This phenomenon for the 2018 period was also studied by Skoczylas-Tworek (2020), who emphasised that the information covered by the statutory obligation includes data on anti-corruption and anti-bribery policies, the results of their application, as well as due diligence procedures binding in this respect, including the risks that may adversely affect them.

Questions arise as to what is the current practice of reporting anti-corruption information, especially with regard to legislative changes that apply to companies starting in 2025 (Ustawa z dnia 29 września 1994…) and how will the companies' experience to date may affect the practice of future reporting.

It is also worth noting that the issue of corruption in terms of reporting information on its prevention appears important from the perspective of state and business security, which in terms of the needs of stakeholders seems obvious. Countries are subject to evaluation within the framework of rankings, and thus in 2024, according to the Corruption Perceptions Index (CPI), Poland scored 53 points on a 100-point scale (100 being the lowest level of corruption perception,

which ranked it 53rd among 180 countries (Transparency International, 2024). The index is a leading global indicator of public sector corruption, providing an annual comparative overview of 180 countries and territories, based on 13 expert assessments and surveys of businesses.

Finally, in the aspect of the conducted research, it is necessary to define the phenomenon of corruption itself, around which all preventive activities of enterprises are initiated, namely corruption in the economic aspect, which within the meaning of Polish law is an act: "committed in the course of business activities involving the performance of obligations to a public authority (institution), consisting in requesting or accepting directly or indirectly by a person in charge of an entity not included in the public finance sector, or working in any capacity for such an entity, any undue benefit or accepting an offer or promise of such benefit to himself or to any other person, in exchange for an action or failure to act that violates his obligations and constitutes socially harmful reciprocation" (Ustawa z dnia 9 czerwca 2006…). In this way it is understood for reporting purposes.

In conclusion, it is worth stressing that in the era of using modern technologies, including artificial intelligence, the challenges facing companies and institutions in terms of sustainability are building an ethical framework for non-financial reporting (De Villiers et al., 2024; Moodaley & Telukdarie, 2023). Survey results, e.g. these of Cumming et al. (2024), confirm that clarity, lack of embezzlement, fairness, explainability, autonomy, privacy and bias require serious attention and postulate trust in algorithms based on a sustainability framework based on artificial intelligence ethics; this certainly influences and justifies the directions of ongoing research in this area.

9.3. Research Methods

The purpose of the survey was to diagnose the situation of companies in terms of reporting anti-corruption information as part of non-financial reporting. The subjects of the study were Polish listed companies (WIG40), and the Orlen Group and Orlen SA were selected for the first stage. The subject covered information on anti-corruption and bribery reported in non-financial information reports from 2017 to 2023 for the selected entities. The realization of the research objective required the use of the following methods: qualitative analysis, synthesis, deduction and induction, comparative analysis, and inference by analogy of phenomena.

The study was conducted based on selected information on anti-corruption (data collection required the development of a research tool in the form of a questionnaire). The research process consisted of a preliminary study (analysis of the case covered by this study, preparation of proposals for the areas to be evaluated for the preparation of the research tool, which was a self-assessment questionnaire) and the study proper (validation of the research tool on a selected entity, diagnosis of the practice of Polish listed companies in the studied scope on the basis of analysis of the content of non-financial reports using the developed questionnaire). In the research process, two hypotheses were verified: (H1) the reporting of information in the field of anti-corruption and bribery increases the information potential of companies and its structure is evolving; (H2) the implementation of non-financial reporting standards into Polish legislation influenced the development of non-financial reporting in the field of anti-corruption and bribery.

In the preliminary study these were verified via the survey of the selected entity (the Orlen Group and Orlen SA). The detailed terms of reference of the research process were as follows:

- development and validation of the research tool,
- a survey proper on a group of listed companies,
- comparative analysis using statistical methods,
- critical discussion and inference by analogy,
- recommendations to the model of information on anti-corruption and bribery, considering the conditions for Polish companies (proposal of indicators).

The realisation of the study required an expert analysis of the scope, type and presentation of information on anti-corruption and bribery disclosed in non-financial reports over the period 2017-2023 by the selected company (case study),included in this study. The adopted hypotheses for the subject of reporting information in the field of anti-corruption and bribery increases the information potential of Orlen Group and Orlen SA and its structure is evolving (`see H1); the implementation of non-financial reporting standards into Polish legislation has influenced the development of non-financial reporting in the field of anti-corruption and bribery of the studied entity (see H2).

9.4. Results

This study qualitatively verified the non-financial information on anti-corruption and bribery in the Orlen Group and Orlen SA from 2017 to 2023. In order to select the most important information for comparison over time, the content of the reports in the area under study was analysed first, the findings are shown in Table 9.1. In accordance with the balance sheet law, the first period for which the company prepared a report on non-financial information was 2017, and the report for this period was only 27 pages long, including only one paragraph on anti-corruption information. It was about minimising the risk of fraud, for which the entity uses a model of three lines of defence. In the first line, risk management was carried out in the operational activities and control mechanisms implemented in the business area. In the second, the compliance of implemented processes with internal regulations was analysed and their risks assessed, whereas the third line was based on auditing and internal control, and supported the functioning of the prevention system (Orlen, n.d.). The company's anti--corruption action system was described in a separate area on risk management, where the types of risks were presented along with their characteristics. It should be noted that disclosures in this aspect, in the same way, were presented in the 2018 report (Table 9.1), but already in its dedicated sections and in an expanded scope.

Table 9.1. Non-financial information on anti-corruption and bribery reported by the Orlen Group and Orlen SA from 2018 to 2023

Type of information	2018	2019	2020	2021	2022	2023
Number of pages in the report	5 pages A4 (53-57)	6 pages A4 (65-70)	9 pages A4 (138-146)	13 pages A4 (219-231)	20 pages A4 (285-304)	20 pages A4 (266-285)
The way the information is presented	narrative description with one diagram and one table	narrative description with one diagram and one table	narrative description with diagrams and drawings (photos)	narrative description by subject area, indicators, tables, diagrams, photos	narrative description by subject area, indicators, tables, diagrams, photos	narrative description by subject area, indicators, tables, diagrams, photos

Characteristics of the area	ensure a fair and transparent business model that guarantees trust, security, free competition and value for all stakeholders	ensure a fair and transparent business model that guarantees trust, security, free competition and value for all stakeholders	ensure a fair and transparent business model that guarantees trust, security, free competition and value for all stakeholders	ensure a fair and transparent business model that guarantees trust, security, free competition and value for all stakeholders	elimination of corrupting factors, compliance with laws and market standards governing anti-corruption and fraud in all markets	no introductory description
Sustainable Development Goals 2030	lacking	lacking	10 – reduces inequalities; 16 – peace, justice and strong institutions	10 – reduces inequalities; 16 – peace, justice and strong institutions	10 – reduces inequalities; 16 – peace, justice and strong institutions	10 – reduces inequalities; 16 – peace, justice and strong institutions
Meters/ indicators – the way to measure (Table 3)	lacking	number of people trained	5 GRI indicators (GRI 103-1; 103-2; 103-3; 205-1; 2025-2)	5 GRI indicators (GRI 103-1; 103-2; 103-3; 205-1; 2025-2)	5 GRI indicators Standards (GRI 11.20.1; 11.20.2; 11.20.3; 11.20.4; 11.20.5)	8 GRI and GRI Oil and Gas Sector (3-3, 11.18.1; 306-3, 11.18.2; 3-3, 11.20.1; 205-1, 11.20.2; 205-2, 11.20.3; 205-3, 11.20.4; 11.20.5, 11.20.6)
Scope from the table of contents (areas)	credo / description of the area / non-financial key performance indicators / description of policies applied / description of due diligence procedures / description of significant business risks and ways to manage risks	credo / description of the area / non-financial key performance indicators / description of policies applied / description of due diligence procedures / description of significant business risks and ways to manage risks	sustainable development goals 2030/ GRI standards indicators credo/ description of the area / non-financial key performance indicators / description of policies in place / description of due diligence procedures / description of material business risks and how risks are managed	description of the area / key non-financial performance indicators / description of policies applied / description of due diligence procedures / description of significant business risks and how risks are managed	management of the anti-corruption and bribery area / key performance indicators / due diligence procedures / significant risks and how to manage them	management of the anti-corruption and bribery area / key performance indicators / due diligence procedures / significant risks and how to manage them
Organisational cells for counteraction and coordination of activities – responsibility	▪ Control and Security Office ▪ Financial Control, Risk Management Risk and Compliance Office ▪ Audit Office	▪ Control and Security Office ▪ Financial Control, Risk Management Risk and Compliance Office ▪ Audit Office	▪ Control and Security Office ▪ Financial Control, Risk Management Risk and Compliance Office ▪ Audit Office	▪ Control and Security Office ▪ Financial Control, Risk Management Risk and Compliance Office ▪ Audit Office	▪ Control and Security Office ▪ Financial Control, Risk Management Risk and Compliance Office ▪ Audit Office	▪ Control and Security Office ▪ Financial Control, Risk Management Risk and Compliance Office ▪ Audit Office

Description of tasks and the scope of their details	narrow scope of tasks without elaborate structures, low level of detail	narrow scope of tasks without elaborate structures, low level of detail	narrow scope of tasks without elaborate structures, low level of detail	wide range of tasks, extensive structure, high degree of detail	wide range of tasks, extensive structure, high degree of detail	wide range of tasks, extensive structure, high degree of detail
Key policies (quantity/form) (Table 2)	14 (miscellaneous form)	17 (miscellaneous form)	17 (miscellaneous form))	18 (miscellaneous form)	16 (miscellaneous form)	22 (miscellaneous form)
The Enterprise Risk Management System (monitored, scheme, 3 lines of defence)	three lines of defence model: 1) Integrated Enterprise Risk Management System; 2) Compliance function and Integrated Management System; 3) Internal audit and control function	three lines of defence model: 1) Integrated Enterprise Risk Management System; 2) Compliance function and Integrated Management System; 3) Internal audit and control function	three lines of defence model: 1) Integrated Enterprise Risk Management System; 2) Compliance function and Integrated Management System; 3) Internal audit and control function	three lines of defence model: 1) Integrated Enterprise Risk Management System; 2) Compliance function and Integrated Management System; 3) Internal audit and control function	three lines of defence model: 1) Integrated Enterprise Risk Management System; 2) Compliance function and Integrated Management System; 3) Internal audit and control function	three lines of defence model: 1) Integrated Enterprise Risk Management System; 2) Compliance function and Integrated Management System; 3) Internal audit and control function
Types of risk (Table 9.4)	(A) Fraud and other Misconduct. (B) Employees' conduct resulting in violation of law. (C) Misconduct on the part of customers or employees	(A) Fraud and other Misconduct. (B) Employees' conduct resulting in violation of law. (C) Misconduct on the part of customers or employees	(A) Fraud and other Misconduct. (B) Employees' conduct resulting in violation of law. (C) Misconduct on the part of customers or employees	(A) Fraud and other Misconduct. (B) Employees' conduct resulting in violation of law. (C) Misconduct on the part of customers or employees	(A) Fraud and other Misconduct. (B) Employees' conduct resulting in violation of law. (C) Misconduct on the part of customers or employees	(A) Fraud and other Misconduct. (B) Employees' conduct resulting in violation of law. (C) Misconduct on the part of customers or employees

Source: own compilation based on analysis of reports on non-financial information from Orlen (n.d.).

As can be seen from the analysis, and also examining the trend of change shown in the table, the scope of information in the subject of the study and the degree of detail over the years has been steadily increasing (the number of pages with presented information is increasing). This is a result of the disclosure of a wider range of information in the analysed area. Although the main organisational units in the surveyed entity responsible for anti-corruption policy did not change, from 2021 the scope of their tasks has increased and their structure has become more complex, as also confirmed by the disclosures of the policies presented. The Orlen Group is developing new, modifying or updating existing policies, regulations, procedures, rules, etc. regarding anti-corruption activities (the scope of internal regulations is systematically increasing or undergoing modification, as detailed in Table 9.2).

Table 9.2. Type of anti-corruption and bribery policies applied by the Orlen Group and Orlen SA from 2018 to 2023

No.	Type of anti-corruption policies	2018	2019	2020	2021	2022	2023
1	Anti-corruption policy	X	X	X	X	–	–
2	Anti-corruption and anti-fraud policy	–	–	–	–	X	X
3	Values and principles of conduct	X	X	X	–	–	–

4	Conflict of interest management policy	–	–	–	X	X	X
5	Code of ethics	–	–	–	X	X	X
6	Compliance policy	–	–	–	–	–	X
7	Anonymous whistleblowing system (AZSN)	X	X	X	X	X	X
8	Gift acceptance and gift giving policy	X Rules	X Rules	X Rules	X Rules	X	X
9	Principles of organising the process of verification of contractors	–	–	–	X	X	X
10	Principles and instructions for countering money laundering and terrorist financing	X	X	X	X	X	X
11	Principles of regulatory risk management as part of compliance policy	X Rules	X Rules	X	X	X	X
12	Principles of corporate governance	X	X	X	X	X	X
13	Code of conduct for suppliers	X	X	X	X	X	X
14	Principles for managing the risk of loss of information security attributes	X	X	X	X	X	X
15	Regulations for conducting financial control	X	X	X	X	X	X
16	Standards for conducting financial audits	–	X	X	X	X	X
17	Regulations for conducting audits, consulting projects and analysis of business activities	X	X	X	X	X	X
18	Corporate risk management policy and procedure	X	X	X	X	X	X
19	Integrated management system policy	X	X	X	X	X	X
20	Rules for the conduct of inspections and verification proceedings	X	X	X	X	–	X
21	Principles of integrated security verification of contractors	–	X	X	X	–	–
22	Principles of monitoring business process security	–	X	X	X	–	–
23	Energy policy	–	–	–	–	–	X
24	Food policy						X
25	Lobbying rules as part of compliance policy						X
26	Principles of concession management as part of compliance policy						X
	Number of regulations in force	**14**	**17**	**17**	**18**	**16**	**22**

Source: own compilation based on analysis of reports on non-financial information from Orlen (n.d.).

The work on internal regulations should be linked to the Orlen Group's implementation of solutions in line with the Sustainable Development Goals (Nos. 10 and 16) from 2020, with the simultaneous application of GRI indicators (GRI, n.d.). The application of non-financial reporting guidelines has increased the comparability of information both over time and within an organisation, as is evident in the surveyed entity, and between different entities that have implemented similar solutions (Szadziewska & Shygun, 2023). The usefulness of the information to stakeholders is enhanced; the use of non-financial indicators makes it possible to assess trends of change in the selected area, as detailed in Table 9.3.

Table 9.3. Measures of information on anti-corruption and bribery (non-financial indicators) in the Orlen Group and Orlen SA from 2019 to 2023

Non-financial indicators used to measure anti-corruption activities by year
2019
No use of indicators. Measure: The number of people trained on-site and through e-learning – 4057 people were trained in the Group, including the Board of Directors. Number of policies applied (17).
2020
GRI 103-1 (Explanation of topics identified as important with an indication of limitations) GRI 103-2 (The approach to governance and its elements in the areas of environmental, social, human rights, anti-corruption ...) GRI 103-3 (Evaluation of the management approach) Measure: Indication of departments, offices, teams, etc. engaged in anti-corruption activities, with an indication of the scope of tasks performed.
GRI 205-1 (Percentage and total number of business units analysed for corruption risks and risks identified) GRI 205-2 (Communication and training on the organisation's anti-corruption policies and procedures) Measure: Number of risks (3 indications – inconsistent in their naming with those listed in the risk management section), including an indication of the number of processes identified in each type of risk (A-35; B-1; C-3). Number of risk assessments carried out at Orlen SA (493), number of controls tested (987) in (145) business processes, similarly, the result in the Group (678) (1818) (171). Use of ERM system – covered (10%) of Group companies. Number of people trained in the subject of the study, (279) employees in classroom mode and (200) people in e-learning training in Orlen SA. Provision of training in e-learning mode. Number of policies (17).
2021
GRI 103-1 (Explanation of topics identified as important with an indication of limitations) GRI 103-2 (Management approach and its elements) GRI 103-3 (Evaluation of the management approach) Measure: Listing of the units operating in the form of departments, offices, teams, etc. dealing with anti-corruption, with an indication of the scope of tasks carried out, their structure.
GRI 205-1 (Percentage and total number of business units analysed for corruption risks and risks identified) GRI 205-2 (Communication and training on the organisation's anti-corruption policies and procedures) Measure: Number of risks (3 - inconsistency in their naming with those listed in the risk management section), including an indication of the number of processes identified in each type of risk (A-34; B-1; C-3). Number of risk assessments conducted at Orlen SA (536), number of controls tested (1002) in (164) business processes, similarly, in the Group (191) (660) (95); ERM system covered 10% of Group companies. The amount of training in the subject of the study, (236) employees of Group companies were trained in stationary mode and 80 in e-learning mode at Orlen SA. Implementation of policies for detection and management of conflicts of interest was implemented through e-learning training – (976) company persons and (31) Group employees. Number of policies (18). 100% of trained individuals.
2022
GRI 11.20.1 (Management of material topic: anti-corruption) Detailed description of the anti-corruption policy in force with characteristics of other internal regulations. Measure: number of policies (16), number of post-inspection orders (177), of which (45) concerned Orlen SA and 132 concerned the Group.
GRI 11.20.2 (Percentage and total number of operations assessed for risks related to corruption; identified risks) Measure: The number of risks (3), including an indication of the number of processes identified in each risk type (A-37; B-24; C-3); the number of risk assessments conducted at Orlen SA (629), the number of tested controls (1027) in (195) business processes, similarly, in the Group (222) (723) (89). The ERM system covered 10% of the Group's companies. Detailed description of actions taken, their scope and location.
GRI 11.20.3 (Communication and training about anti-corruption policies and procedures) Measure: Indication in percentage terms of internal audiences to whom anti-corruption policies and procedures have been presented (100%) of governing bodies, employees, business partners, indication in percentage terms of people who have been trained in this area (100%).

GRI 11.20.4 (Confirmed incidents of corruption and actions taken) Measure: The total number and nature of cases of corruption, dismissals for this reason, termination of contracts and court cases, in each case the Group found none.
GRI 11.20.5 (Transparency of contracts and licences) Measure: The descriptive form stating that policies are implemented to ensure transparency in contracting, implementation of audits, without reference to quantitative or percentage.
2023
GRI 3-3 GRI 11.20.1 (management of material topic: anti-corruption) Detailed description of the anti-corruption policy in force with characteristics of other internal regulations. Measure: number of policies (22).
GRI 3-3 GRI 11.18.1 (Managing a relevant topic: conflicts and security) Description of security regulations and reference to risk management in this regard.
GRI 11.18.2 (Percentage of personnel responsible for ensuring security trained in the organisation's policies and procedures on various aspects of human rights related to its operations.) Measure: 100% of security personnel have familiarised themselves with the Code of Ethics and Regulations against Bullying, Discrimination and All Forms of Harassment. The indicator monitoring the process of improving staff preparation increased from (82.67%) in 2022 to (83.29%).
GRI 11.20.2 (Percentage and total number of operations assessed for risks related to corruption; identified risks) Measure: Number of risks (3), including an indication of the number of processes identified in each type of risk (A-36; B-23; C-3). The number of risk assessments conducted at Orlen SA (521), the number of tested controls (992) in (165) business processes, similarly, in the Group (638) (1607) (183). The ERM system covered 10% of the Group's companies. Detailed description of actions taken, their scope and location.
GRI 11.20.3 (Communication and training about anti-corruption policies and procedures) Measure: Indication in percentage terms of internal audiences to whom anti-corruption policies and procedures were presented (100%) governing bodies, employees, business partners, indication in percentage terms of people who were trained in this area (100%).
GRI 11.20.4 (Confirmed incidents of corruption and actions taken) Measure: The total number and nature of corruption cases, dismissals for this reason, termination of contracts. One court case against employees under Art. 305 of the Criminal Code (the company has the status of a victim). In each case, the Group found none.
GRI 11.20.5 (Transparency of contracts and licences) Measure: Use of Dok-system. The contracting procedure, the draft contract, is coordinated with various units, including legal, finance, tax and controlling departments, before being concluded.
GRI 11.20.6 (List of actual owner-beneficiaries) Measure: Rules for organising the process of verification of contractors.

Source: own compilation based on analysis of reports on non-financial information from the ORLEN (n.d.).

As can be seen from the analysis of the content presented in the table, the use of numerical, percentage, or possibly descriptive metrics (in accordance with the GRI guidelines) increases the comparability of information, enables an objective assessment of the entity's activities in each area, and enhances the transparency of the entity, which can translate into the way it is perceived by stakeholders. It is worth noting that this area of surveyed information has been significantly modified, but will require further standardisation. This justifies the need for continued research, and the evaluation of the reporting practices of other entities could enable the development of an information model in the area of anti-corruption measures taken. Reliability, comprehensibility, and comparability of information could increase business security, contributing to stakeholder confidence.

Risk management is another important topic area regarding the entity's activity in applying the anti-corruption policy. The Orlen Group has been identifying three types of risks since 2018, and from 2019 their characteristics are still developing, slightly affecting their overall

perception. A greater change in the reporting of risk information is evident in reports prepared from 2020. The measurement of risks, the assessment of their materiality, the changes after the application of control mechanisms and the probability of their occurrence are presented in the study, and the information is shown in tables and figures. Details can be seen in Table 9.4. The report also presents a detailed structure of the risk management system, along with the roles that each unit plays in the system.

Table 9.4. Information on Orlen SA's risk management against corruption and bribery

Risk description	2018	2019	2020	2021	2022	2023
Fraud and other Misconduct (A)						
Detailed characteristics of the risk	Accepting financial benefits property from potential suppliers. Conflict of interest in making transactions.	Accepting financial benefits property from potential suppliers. Conflict of interest in making deals. Disclosure of confidential information. Falsification of information management or other documents.	Accepting financial benefits property from potential suppliers. Conflict of interest in making deals. Disclosure of confidential information. Falsification of information management or other documents.	Accepting financial benefits property from potential suppliers. Conflict of interest in making deals. Disclosure of confidential information. Falsification of information management or other documents.	Accepting financial benefit property from potential suppliers. Conflict of interest in making deals. Disclosure of confidential information. Falsification of information management or other documents.	Accepting financial benefits property from potential suppliers. Conflict of interest in making deals. Disclosure of confidential information. Falsification of information management or other documents.
Risk mitigation methods	Limited access to bids, monitoring of confirmation of impartiality to potential suppliers, supervision of the path acceptance path of supplier selection.	Methods of 2018, in addition, regulated and limited access to company-secret information, procedures for verifying documentation and management information.	Methods of 2018, in addition, regulated and limited access to company-secret information, procedures for verifying documentation and management information.	Methods of 2018, in addition, regulated and limited access to company-secret information, procedures for verifying documentation and management information.	Methods of 2018, in addition, regulated and limited access to company-secret information, procedures for verifying documentation and management information.	Methods of 2018, in addition, regulated and limited access to company-secret information, procedures for verifying documentation and management information.
Risk development trend	–	–	stable	stable	stable	stable
Materiality – the level of risk	–	–	average	average	average	average
The level of risk taking into account the control mechanisms used	–	–	low	low	low	low
Probability of occurrence	–	–	decrease (2-2)	decrease (2-2)	decrease (2-2)	decrease (2-2)

Employees' conduct resulting in the violation of law (B)						
Detailed characteristics of the risk	Involvement in the conclusion of illegal transactions or their by employees. Entering into contracts in situations, in which regulations do not allow the process to continue.	Involvement in the conclusion of illegal transactions or their by employees. Entering into contracts in situations, in which regulations do not allow the process to continue.	Involvement in the conclusion of illegal transactions or their by employees. Entering into contracts in situations, in which regulations do not allow the process to continue.	Involvement in the conclusion of illegal transactions or their by employees. Entering into contracts in situations, in which regulations do not allow the process to continue.	Involvement in the conclusion of illegal transactions or their by employees. Entering into contracts in situations, in which regulations do not allow the process to continue.	Involvement in the conclusion of illegal transactions or their by employees. Entering into contracts in situations, in which regulations do not allow the process to continue.
Risk mitigation methods	Verification of the correctness of obligations incurred with the powers of attorney held, supervision of contracts with suppliers and the level of security of the Group's interests groups.	Verification of the correctness of obligations incurred, with the powers of attorney held, supervision of contracts with suppliers and the level of security of the Group's interests group. Opinion and approval of contracts by business areas in the system.	Verification of the correctness of obligations incurred with the powers of attorney held, supervision of contracts with suppliers and the level of security of the Group's interests group. Opinion and approval of contracts by business areas in the system.	Verification of the correctness of obligations incurred with the powers of attorney held, supervision of contracts with suppliers and the level of security of the Group's interests group. Opinion and approval of contracts by business areas in the system.	Verification of the correctness of obligations incurred with the powers of attorney held, supervision of contracts with suppliers and the level of security of the Group's interests group. Opinion and approval of contracts by business areas in the system.	Verification of the correctness of obligations incurred with the powers of attorney held, supervision of contracts with suppliers and the level of security of the Group's interests group. Opinion and approval of contracts by business areas in the system.
Risk development trend	–	–	stable	stable	stable	stable
Materiality – the level of risk	–	–	average	average	average	average
The level of risk taking into account the control mechanisms used	–	–	low	low	low	low
Probability of occurrence	–	–	Significant reduction (3-2)	Significant reduction (3-2)	Significant reduction (3-2)	Significant reduction (3-2)
Misconduct on the part of customers or employees (C)						
Detailed characteristics of the risk	Theft of fuels by employees/ customers. Release of products to unauthorised persons, to unauthorised vehicles	Theft of fuels by employees/ customers. Release of products to unauthorised persons, to unauthorised vehicles	Theft of fuels by employees/ customers. Release of products to unauthorised persons, to unauthorised vehicles	Theft of fuels by employees/ customers. Release of products to unauthorised persons, to unauthorised vehicles	Theft of fuels by employees/ customers. Release of products to unauthorised persons, to unauthorised vehicles	Theft of fuels by employees/ customers. Release of products to unauthorised persons, to unauthorised vehicles

Risk mitigation methods	Periodic inspections of fuel stations and terminals, overseeing the ordering and issuance of product awards in accordance with regulations.	Periodic inspections of fuel stations, terminals, verification and monitoring of reports on compliance. Automatic process of blocking and unblocking of sales orders for customers.	Periodic inspections of fuel stations, terminals, verification and monitoring of reports on compliance. Automatic process of blocking and unblocking of sales orders for customers.	Periodic inspections of fuel stations, terminals, verification and monitoring of reports on compliance. Automatic process of blocking and unblocking of sales orders for customers.	Periodic inspections of fuel stations, terminals, verification and monitoring of reports on compliance. Automatic process of blocking and unblocking of sales orders for customers.	Periodic inspections of fuel stations, terminals, verification and monitoring of reports on compliance. Automatic process of blocking and unblocking of sales orders for customers
Risk development trend	–	–	stable	stable	failing	stable
Materiality – the level of risk	–	–	average	average	average	average
The level of risk taking into account the control mechanisms used	–	–	low	low	low	low
Probability of occurrence	–	–	significant reduction (3-2)	significant reduction (3-2)	constant (1-1)	constant (1-1)

Source: own compilation based on analysis of reports on non-financial information from Orlen (n.d.).

Analysing the content of the table, one can see a trend of change similar to that in other areas, with the scope of disclosure being limited in the first periods, then increasing to take a stable form from 2020 onwards. The apparent stability in the approach to risk management means that in the Orlen Group the policy in this area has been formed and has not changed for years. This raises the question of whether, along with a change in the approach to corporate reporting, there should be a change in the approach to managing the risk of corruption fraud, or would this area similarly be monitored and controlled, whether there was an obligation to report it or not? However, a good signal, worth reiterating, is the changes in internal regulations. The entity regularly updates policies, takes into account changes resulting from external legislative changes and observations of other entities' practices. It should be remembered that the mere quantity of these does not necessarily imply quality, and the mere development of them does not necessarily imply their implementation, hence it would be worthwhile to measure the degree of implementation of such solutions. The question remains whether this would translate into risk minimisation and greater efficiency, thereby contributing to preventive action, preventing these phenomena. The fact is that with reliable reporting, the revealed issue can be investigated, monitored, analysed, and evaluated, which is important for the business environment.

Finally, note that the qualitative analysis of the report content should be complemented by an analysis and evaluation of the way the information is presented, in which narrative description predominates, over time supplemented by diagrams, tables, figures, which also increases the number of pages in the report. Effective communication with stakeholders requires greater flexibility as to the variety of forms of content presentation (narrative, numerical, pictorial). Stakeholders' information needs are different, as well as their

knowledge, experience, skills, sensitivity to perception. Meeting these needs therefore becomes crucial to effective communication.

9.5. Discussion

The analysis and evaluation of the content of the reports enabled the hypotheses set for the study to be adopted. According to the author, the reporting of information on counteracting corruption and bribery increases the information potential of the examined entity and its structure is evolving, and this development was influenced by non-financial reporting standards implemented in the Polish legislation. The objective of diagnosing the anti-corruption information reporting practice of the selected entity (Orlen Group and Orlen SA) was achieved. For the results of the study to be representative and for the diagnosis of reporting practices to include other industries and a representative research sample, conclusions and recommendations were formulated.

Conclusions from the analysis of the case study made it possible to identify aspects of non--financial reporting on anti-corruption subject to the assessment, considered when building the assessment questionnaire (research tool) used to collect data in the next stage of the study, to include:

- analysis of the number of disclosures in each area, together with the change in the number of disclosures of the other areas of information and of the report as a whole (number of pages, number of characters, percentage range – possibility of examining a trend);
- analysis of the degree of compliance – examination of the compliance of non-financial reports with the guidelines in terms of the applicable legislation;
- analysis of the types of internal regulations in the field of anti-corruption and the degree of their implementation (number, links, assessment of the degree of implementation, e.g. in percentage terms);
- evaluation of the type of thematic areas with detailed analysis of the way the information is presented (qualitative study in terms of evaluation of the degree of comprehensibility, clarity, usefulness, and forms of presentation – narrative description, numerical, tabular, graphic – photos, drawings, diagrams, according to the adopted scale);
- analysis of the degree of detail of the information (qualitative analysis according to the adopted scale, e.g. evaluation scale 1-5, where 1 – the degree of detail of the information is the lowest, 5 – the degree of detail is the highest);
- evaluation of the type and scope of indicators used in relation to the GRI standards (measuring the effects of the implementation of the anti-corruption policy – type of indicators, measures and units used).

It is recommended that a universal information model is developed around anti-corruption, the implementation of which in the non-financial reporting of entities from different industries, with different specificities of activity increasing the usefulness of non-financial reporting.

Finally, it should be emphasised that an assessment of the reliability of the presented information is not possible based on the reporting alone, it requires an examination of the entity through the prism of other information to which access is not always possible. Hence the introduction of an obligation to examine non-financial information carried out by audit firms or to assess the entity's reputation in the economic market. The example of the Orlen Group companies and Orlen SA itself, entities subjected to evaluation in the eyes of experts and the public, appears to be an appropriate example in the context of the possibility to

compare the adopted subjective opinions with the anti-corruption information that the company publishes in its reports.

9.6. Conclusions

The conclusions of the preliminary study allow for the adoption of the hypotheses set for the studied entity and are necessary for the study proper, the purpose of which was realised, the reporting practice for the selected entity diagnosed, whilst the information areas and the way to evaluate them in the proper study were proposed, and the solutions for reporting anti--corruption information recommended, however the disclosures were not always sufficient for the environment and do not always meet the information requirements of stakeholders. The research continues on a group of Polish listed companies, and the conclusions of this study provide the basis for further analysis and evaluation, the results of which will be published in the next study. It is also acknowledged that examining only entities from Poland may be a limitation, hence the recommendation to conduct the analysis on analogous groups of companies from other countries, in particular the Visegrád countries (4V).

In conclusion, it is important to stress that the results from the survey have socio-economic relevance, because corruption negatively affects economic development and social trust. These can be translated into non-financial reporting practices in other countries with similar development conditions (for example, the 4V countries), using the same survey questionnaire. The anti-corruption diagnosis presented in the non-financial reports supports the building of a more ethical business environment. Additionally, in terms of application, the diagnosis of the situation will identify a gap in reporting, but also reveal good reporting practices exemplary for other companies. This is particularly important in the context of the legislative changes introduced for Polish enterprises. The European Union published the CSRD Directive which entered into force in January 2023. In Poland this was implemented into the Polish legal order as of 1 January 2025 in accordance with the provisions of the Act of 17 December 2024 on the amendment of the Accounting Act, the Act on Statutory Auditors, Audit Firms and Public Supervision and some other acts (Ustawa z dnia 29 września 1994…), which are the most recent at this point. This will translate into transparency as a value, on non-financial sustainability reporting issues, expected from companies by their stakeholders.

References

Aldaz, M., Alvarez, I., & Calvo, J. A. (2015). Non-Financial Reports, Anti-Corruption Performance and Corporate Reputation. *Revista Brasileira de Gestao de Negocios*, *17*(58), 1321-1340. https://doi.org/10.7819/rbgn.v17i58.2687

Aluchna, M., Kamiński, B., & Wrzosek, M. (2024). Anti-Corruption Disclosure: Evidence from the Natural Experiment of the Non-Financial Reporting Directive. *DECISION*, *51*(2), 165-182. https://doi.org/10.1007/s40622-024-00386-z

Baboukardos, D., Gaia, S., Lassou, P., & Soobaroyen, T. (2023). The Multiverse of Non-Financial Reporting Regulation. *Accounting Forum*, *47*(2), 147-165. https://doi.org/10.1080/01559982.2023.2204786

Bąk, M., Strojek-Filus, M., Kobiela-Pionnier, K., & Masztalerz, M. (2022). *Narracje w sprawozdawczości finansowej i niefinansowej*. Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu.

Bek-Gaik, B., & Surowiec, A. (2020). *Informacje niefinansowe w sprawozdawczości organizacji*. CeDeWu.

Błażyńska, J. (2018). Reporting Non-Financial Information. *Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu*, (503), 59-67. https://doi.org/10.15611/pn.2018.503.05

Carmo, C., & Ribeiro, C. (2022). Mandatory Non-Financial Information Disclosure Under European Directive 95/2014/EU: Evidence from Portuguese Listed Companies. *Sustainability*, *14*(8), Article 4860. https://doi.org/10.3390/su14084860

Cumming, D., Saurabh, K., Rani, N., & Upadhyay, P. (2024). Towards AI Ethics-Led Sustainability Frameworks and Toolkits: Review and Research Agenda. *Journal of Sustainable Finance and Accounting*, *1*, Article 100003. https://doi.org/10.1016/j.josfa.2024.100003

De Villiers, C., Dimes, R., & Molinari, M. (2024). How Will AI Text Generation and Processing Impact Sustainability Reporting? Critical Analysis, a Conceptual Framework and Avenues for Future Research. *Sustainability Accounting, Management and Policy Journal*, *15*(1), 96-118. https://doi.org/10.1108/SAMPJ-02-2023-0097

European Union. (2014). Sprostowanie do dyrektywy Parlamentu Europejskiego i Rady 2014/95/UE z dnia 22 października 2014 r. zmieniającej dyrektywę 2013/34/UE w odniesieniu do ujawniania informacji niefinansowych i informacji dotyczących różnorodności przez niektóre duże jednostki oraz grupy (Dz.U. L 330 z 15.11.2014). https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32014L0095R(02)

GRI. (n.d.). *The Global Leader for Sustainability Reporting*. https://www.globalreporting.org

Krasodomska, J., Śnieżek, E., & Szadziewska, A. (2018). *Informacje niefinansowe w sprawozdawczości biznesowej przedsiębiorstw*. Wydawnictwo Nieoczywiste.

Landis, C., & Paglietti, P. (2024). Legitimacy and Anti-Corruption Disclosures: Insights into the Early Effects of the European Non-Financial Reporting Directive. *Journal of Accounting and Organizational Change*. https://doi.org/10.1108/JAOC-04-2023-0077

Matuszak, Ł., & Różańska, E. (2017). CSR Disclosure in Polish-listed Companies in the Light of Directive 2014/95/EU Requirements: Empirical Evidence. *Sustainability*, *9*(12), Article 2304. https://doi.org/10.3390/su9122304

Matuszak, Ł., & Różańska, E. (2021). Towards 2014/95/EU Directive Compliance: The Case of Poland. *Sustainability Accounting, Management and Policy Journal*, *12*(5), 1052-1076. https://doi.org/10.1108/SAMPJ-02-2020-0042

Mbanyele, W., Huang, H., Li, Y., Muchenje, L. T., & Wang, F. (2022). Corporate Social Responsibility and Green Innovation: Evidence from Mandatory CSR Disclosure Laws. *Economics Letters*, *212*, Article 110322. https://doi.org/10.1016/j.econlet.2022.110322

Moodaley, W., & Telukdarie, A. (2023). Greenwashing, Sustainability Reporting, and Artificial Intelligence: A Systematic Literature Review. *Sustainability*, *15*(2). https://doi.org/10.3390/su15021481

Mysaka, H., & Derun, I. (2024). A Bibliometric Analysis of the Impact of Theoretical Frameworks on EU Directives: The Case of Sustainability Reporting and Non-Financial Reporting. *Zeszyty Teoretyczne Rachunkowosci*, *48*(4), 75-96. https://doi.org/10.5604/01.3001.0054.8690

Orlen. (n.d.). *Raporty i publikacje: Sprawozdania*. https://www.orlen.pl/pl/relacje-inwestorskie/raporty-i-publikacje/sprawozdania

Roberts, C., Gordon, P., & Weetman, P. (2008). *International Corporate Reporting: A Comparative Approach*. Prentice Hall/Financial Times.

Skoczylas-Tworek, A. (2020). Disclosure of Non-Financial Information in the Field of Counteracting Corruption and Bribery in Economic Practice. *Prace Naukowe Uniwersytetu Ekonomicznego We Wrocławiu*, *64*(4), 187-198. https://doi.org/10.15611/pn.2020.4.14

Szadziewska, A., & Shygun, M. (2023). The Use of Infographics for Impression Management in the Non-Financial Reports of Listed Companies in Poland. *Zeszyty Teoretyczne Rachunkowosci*, *47*(2), 51-80. https://doi.org/10.5604/01.3001.0053.6059

Transparency International. (2024). *Corruption Perceptions Index*. https://www.transparency.org/en/cpi/2024

Turzo, T., Marzi, G., Favino, C., & Terzani, S. (2022). Non-Financial Reporting Research and Practice: Lessons from the Last Decade. *Journal of Cleaner Production*, *345*, Article 131154. https://doi.org/10.1016/j.jclepro.2022.131154

Ustawa z dnia 29 września 1994 r. o rachunkowości (Dz. U. 2023 poz. 120, 295, 1598, 2024 poz. 619, 1685, 1863.).

Ustawa z dnia 9 czerwca 2006 o Centralnym Biurze Antykorupcyjnym (Dz. U. 2021 poz. 1671, 2333, 2022 poz. 1488.).

Yadav, S., Samadhiya, A., Kumar, A., Luthra, S., & Pandey, K. K. (2024). Environmental, Social, and Governance (ESG) Reporting and Missing (M) Scores in the Industry 5.0 Era: Broadening Firms' and Investors' Decisions to Achieve Sustainable Development Goals. *Sustainable Development*. https://doi.org/10.1002/sd.3306

Chapter 10

Recommendations for Combating Corruption and Fraud: Insights from the V4 and Ukraine

Piotr Luty

Wroclaw University of Economics and Business
ORCID: 0000-0003-0955-7000

Quote as: Luty, P. (2025). Recommendations for Combating Corruption and Fraud: Insights from the V4 and Ukraine. In I. Chuy, P. Luty, V. Lakatos (Eds.), *Modern Tools for Fraud Detection: Insights from the V4 and Ukraine* (pp. 120-123). Publishing House of Wroclaw University of Economics and Business.

DOI: 10.15611/2025.40.5.10

10.1. Introduction

The project aimed to share the knowledge of the Visegrad Group countries and Ukraine in fighting corruption, counteracting fraud and money laundering. During the implementation of the project, three seminars were held, and three monographs created – this is the last of them. Based on scientific research and publications contained in these monographs, recommendations can be made in seven areas: fighting corruption, fighting CIT fraud, fighting PIT fraud, fighting money laundering, fight other types of fraud, AI and fight against corruption and fraud, and modern tools for fighting corruption and fraud. The recommendations resulting from the research of the project participants are presented below.

10.2. Fight Against Corruption

Corruption remains a significant impediment to economic stability, public trust, and institutional effectiveness in both Visegrad Group (V4) countries and Ukraine. Despite notable anti--corruption reforms such as Ukraine's Prozorro public procurement system and the establishment of anti-corruption bodies e.g. NACP (National Agency on Corruption Prevention) and NABU (National Anti-Corruption Bureau of Ukraine), systemic corruption persists due to entrenched political and economic interests (Luty et al., 2024).

To effectively combat corruption, the following strategies are recommended.

- **Strengthening Legal and Institutional Frameworks:** governments must ensure the independence of judicial institutions and enforcement agencies. Legal reforms should focus on increasing the efficiency of anti-corruption investigations and ensuring the swift prosecution of corruption cases.

- **Enhancing Transparency and Public Participation:** digital public procurement systems should be expanded and improved to reduce opportunities for bribery and favouritism. Countries should adopt real-time monitoring tools to track public expenditure.
- **Anti-Corruption Education and Awareness:** awareness campaigns targeting public officials, businesses, and citizens can foster a culture of integrity. Ethical training programmes in public administration can also reduce the tolerance for corruption.
- **Whistleblower Protection:** stronger legal protections should be provided for whistleblowers to encourage the reporting of corrupt practices without fear of retaliation (Luty et al., 2024).

10.3. Fight Against Corporate Income Tax (CIT) Fraud

CIT fraud, including **profit shifting, transfer pricing manipulation, and tax evasion through offshore entities**, remains a significant issue in the V4 countries and Ukraine (Balytska et al., 2025). Practical strategies to counter CIT fraud include (Chuy et al., 2025):

- **Strengthening International Tax Cooperation:** aligning national tax regulations with OECD's BEPS (Base Erosion and Profit Shifting) framework can help limit aggressive tax planning.
- **Enhancing Transfer Pricing Controls:** governments should implement stricter transfer pricing regulations requiring detailed documentation of intra-group transactions.
- **Data-Driven Tax Audits:** AI-powered data analytics can identify inconsistencies in financial reporting and detect suspicious tax practices.
- **Tax Reporting Transparency:** public disclosure of corporate tax contributions can discourage aggressive tax avoidance schemes.

10.4. Fight Against Personal Income Tax (PIT) Fraud

Personal income tax fraud primarily manifests as undeclared income, false deductions, and disguised employment relationships (e.g. the Švarc systém in Czechia, see (Balytska et al., 2025)). Measures to combat PIT fraud include:

- **Progressive Taxation and Simplified Reporting:** moving toward a progressive tax system and reducing administrative complexities can encourage voluntary compliance.
- **Enhanced Digital Monitoring:** integrating electronic payroll systems and digital tax filings can improve the detection of undeclared earnings.
- **Penalties and Incentives:** while increasing penalties for tax evasion is necessary, providing incentives such as tax amnesty programmes can encourage individuals to declare previously hidden income.

10.5. Fight Against Money Laundering

The fight against money laundering has gained prominence, particularly in Ukraine, where the war has increased the risks related to financial crime and terrorist financing (Balytska et al., 2025). Recommendations include:

- **Implementing Blockchain-Based Solutions:** blockchain technology enables the real-time tracking of financial transactions, reducing the ability to launder money through complex financial networks.
- **Enhancing International Cooperation:** stronger collaboration with Europol, FATF (Financial Action Task Force), and the European Commission can facilitate information sharing and coordinated enforcement actions.
- **Stricter AML (Anti-Money Laundering) Compliance for Cryptocurrencies:** governments should impose Know Your Customer (KYC) and transaction monitoring requirements on cryptocurrency exchanges.
- **Advanced AI and Machine Learning Tools:** AI-driven financial crime monitoring systems can detect suspicious patterns in banking transactions.

10.6. Fight Against Other Types of Fraud (VAT Fraud, Financial Statement Manipulation, and Fraudulent Business Practices)

VAT fraud, particularly carousel fraud**,** results in billions of euros in lost tax revenue across the EU (Chuy et al., 2025). Additionally, creative accounting and fraudulent business practices undermine financial stability. Strategies to mitigate these issues include:

- **Expanding Reverse Charge Mechanisms:** the domestic reverse charge system has successfully prevented fraudulent VAT refunds in high-risk sectors (e.g. fuel trade in the Czech Republic).
- **Real-Time Invoice Verification:** implementing automated VAT reporting and e-invoicing systems can significantly reduce fraud risks.
- **Strengthening Financial Audits:** regulators should enforce mandatory external audits for companies operating in fraud-prone industries.
- **Public Transparency Measures:** encouraging companies to disclose non-financial information, including anti-corruption policies, can deter fraudulent practices.

10.7. AI and the Fight Against Corruption and Fraud

Artificial Intelligence (AI) is a transformative tool for fraud detection, capable of analysing vast datasets in real-time and identifying patterns indicative of fraud (Chuy et al., 2025). Key AI--driven approaches include:

- **AI-Powered Risk Assessments:** machine learning algorithms can assess the likelihood of fraud based on historical data and risk indicators.
- **Blockchain for Fraud Prevention:** distributed ledger technology can improve the transparency of financial transactions and public procurement processes.
- **AI-Powered Whistleblower Platforms:** secure AI-driven reporting systems can facilitate the anonymous submission of fraud-related evidence.
- **Automated Compliance Systems:** AI can automatically flag suspicious financial transactions, tax declarations, and procurement bids.

10.8. Modern Tools for Fighting Corruption and Fraud

Several modern tools have proved to be effective in the fight against financial crime and corruption (Balytska et al., 2025; Chuy et al., 2025; Luty et al., 2024). The most promising include:

- **Big Data Analytics:** governments should leverage large-scale data analysis to detect inconsistencies in tax filings, procurement records, and financial statements.
- **Electronic Public Procurement Platforms:** expanding systems such as Prozorro can improve transparency in government contracting.
- **AI-Driven Tax Compliance Platforms:** countries should invest in real-time tax monitoring and automated compliance systems to reduce fraud.
- **RegTech and SupTech Solutions:** regulatory technology (RegTech) and supervisory technology (SupTech) can help financial regulators detect fraud faster and ensure compliance with AML laws.
- **Cross-Border Data Sharing Agreements:** establishing secure data exchange mechanisms between tax administrations and financial intelligence units across Europe can enhance fraud prevention efforts.

10.9. Conclusions

The fight against corruption and fraud requires a multi-faceted approach, combining legislative reforms, digital innovations, and international cooperation. Lessons from the V4 countries and Ukraine demonstrate that while progress has been made, there is still significant room for improvement in tax enforcement, corporate transparency, and anti-money laundering efforts. By adopting AI-driven solutions, blockchain technology, and cross-border regulatory frameworks, the authorities can strengthen fraud prevention and ensure economic stability.

References

Balytska, M., Bohušová, H., & Luty, P. (Eds.). (2025). *The V4 and Ukraine Fight with Tax Fraud and Money Laundering*. Publishing House of Wroclaw University of Economics and Business.

Chuy, I., Luty, P., & Lakatos, V. (Eds.). (2025). *Modern Tools for Fraud Detection: Insights from V4 and Ukraine*. Publishing House of Wroclaw University of Economics and Business.

Luty, P., Versal, N., & Semerád, P. (Eds.). (2024). *Knowledge and Digitalisation Against Corruption and Fraud*. Publishing House of Wroclaw University of Economics and Business.

Afterword

Fraud remains a major challenge for governments, businesses, and financial institutions worldwide. This book provides an in-depth exploration of modern tools and strategies for fraud detection, focusing on insights from the Visegrad Four (V4) countries – Poland, Czechia, Hungary, Slovakia – and Ukraine. Throughout eight chapters, it examines tax fraud, occupational fraud, financial manipulation, and corruption, highlighting innovative technologies, regulatory challenges, and policy recommendations.

The Role of AI in Tax Fraud Detection – modern technologies such as artificial intelligence (AI), blockchain, and predictive analytics are revolutionising tax fraud detection. AI-powered solutions enable real-time anomaly detection, automated risk assessments, and cross-border data verification, significantly improving tax enforcement efficiency. However, AI alone is not a complete solution – it must be complemented by human oversight to ensure accuracy, fairness, and legal compliance. The integration of AI with expert auditing can strengthen tax compliance, reduce administrative burdens, and promote fiscal transparency.

Ukraine faces significant tax security challenges, including widespread tax evasion through grey imports, smuggling, and under-the-table salaries. The COVID-19 pandemic and the ongoing war have further strained tax revenue stability. Strengthening tax security requires a multi-faceted approach: reducing the tax burden on labour, increasing fiscal oversight, improving tax administration efficiency, and enhancing anti-evasion measures. Reforming tax authorities, introducing progressive taxation, and fostering a culture of voluntary compliance are key steps toward a more resilient tax system.

Occupational fraud poses a major threat to organisations in the V4 region and Ukraine, affecting financial stability, corporate reputation, and operational security. The most common types of fraud include asset misappropriation, corruption, and financial reporting manipulation. While whistleblowing systems and advanced analytics have improved fraud detection rates, significant gaps remain in internal controls, legal frameworks, and resource allocation. Strengthening anti-fraud mechanisms, increasing awareness, and adopting AI-driven fraud detection tools are critical to mitigating occupational fraud risks.

Creative accounting, or the manipulation of financial statements, distorts the true financial health of companies and undermines market integrity. While such practices can offer short--term financial advantages, they pose long-term risks, including legal penalties, loss of investor confidence, and financial instability. The widespread use of creative accounting in Czechia highlights the need for stricter regulatory oversight and better financial reporting transparency. New technologies, such as data analytics and forensic accounting tools, can help detect and prevent financial misrepresentation.

The ability of tax authorities to block bank accounts raises significant concerns regarding legal safeguards and the economic consequences. While intended to prevent tax evasion and money laundering, account blocking measures often lack transparency and can disrupt legitimate business operations. In Poland, recent legal rulings have clarified the responsibility of tax authorities and financial institutions, emphasising the need for procedural fairness. Greater legal certainty, improved oversight mechanisms, and clearer guidelines for account blocking procedures are necessary to protect taxpayers' rights.

Value Added Tax (VAT) fraud, particularly carousel fraud, remains a significant problem within the European Union, causing billions in lost tax revenue annually. Czechia and the other V4 countries have implemented mechanisms such as VAT control statements, domestic reverse charge, and transaction monitoring to combat fraudulent schemes. However, fraudsters continually adapt to new regulations, exploiting legal loopholes and weak enforcement. Effective VAT fraud prevention requires a combination of legislative reforms, enhanced international cooperation, and stricter due diligence by businesses.

Corporate non-financial reporting plays a crucial role in strengthening transparency and anti--corruption efforts. A study of Polish listed companies revealed significant gaps in anti-corruption disclosures, highlighting the need for standardised reporting practices. The implementation of the EU's Corporate Sustainability Reporting Directive (CSRD) is expected to improve corporate accountability and provide stakeholders with clearer insights into anti-corruption measures. Enhanced regulatory frameworks and increased public awareness can drive ethical business practices and reduce corruption risks.

This book underlines the importance of modernising fraud detection strategies through the adoption of new technologies, improved legal frameworks, and stronger institutional cooperation. While AI, blockchain, and big data analytics offer promising solutions, they must be integrated with traditional auditing and regulatory oversight to be fully effective. The experiences of the V4 countries and Ukraine provide valuable lessons for other economies facing similar fraud-related challenges.

Moving forward, policymakers, financial institutions, and businesses must prioritise proactive fraud prevention measures. Strengthening international collaboration, investing in advanced fraud detection technologies, and fostering a culture of compliance are essential in combating financial crimes and ensuring long-term economic stability.

Acknowledgements

I would like to express my sincere gratitude to the entire team of the Project Management Center for their support throughout the implementation of this project – their commitment and collaborative spirit have been invaluable to its success.

I am particularly grateful to Joanna Mrozek (the Project Manager) and Marta Wasilewska (the previous Project Manager) for their involvement, professionalism, and unwavering support at every stage of the project.

Thank you all for your hard work and contribution.

List of Figures

List of Tables

Visegrad Fund

The project is co-financed by the Governments of Czechia, Hungary, Poland and Slovakia through Visegrad Grants from International Visegrad Fund. The mission of the fund is to advance ideas for sustainable regional cooperation in Central Europe

Project partners

Mendelova univerzita v Brně

Ambis.

Universitas Presoviensis 1667 1997

University of Debrecen

Київський національний університет імені Тараса Шевченка

University of Economics and Business Prague

Львівський торговельно-економічний університет

Stowarzyszenie Księgowych w Polsce
Oddział Dolnośląski we Wrocławiu

The project "Experience sharing of V4 against the shadow economy, corruption and tax avoidance in Ukraine" is co-financed by the Governments of Czechia, Hungary, Poland and Slovakia through Visegrad Grants from International Visegrad Fund. The mission of the fund is to advance ideas for sustainable regional cooperation in Central Europe.

Our books can be read on:
ibuk.pl and ebookpoint.pl

The address of the editor:

Publishing House of Wroclaw University of Economics and Business
53-345 Wrocław, ul. Komandorska 118/120
www.wydawnictwo.uew.pl

Orders:
tel. 71 36 80 602, e-mail: econbook@ue.wroc.pl
ksiegarnia.ue.wroc.pl

ISBN 978-83-68394-40-5