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