DOI: 10.55643/ser.2.56.2025.606

Iryna Mihus
D.Sc. in Economics, Professor, Visiting Professor of the Pontifical Catholic University of Paraná, Curitiba, Brazil; Director of the Scientific Center of Innovative Research, Estonia; Professor of the Department of Financial and Economic Security Management, "KROK" University, Kyiv, Ukraine;
e-mail: irynamihus@gmail.com
ORCID: 0000-0001-6939-9097

Received: 05/04/2025
Accepted: 19/06/2025
Published: 30/06/2025

FRAUD HUNTERS AROUND THE WORLD: FIGHTING DECEPTION IN DIFFERENT COUNTRIES

ABSTRACT

As financial fraud grows more sophisticated and global in scope, countries have developed diverse mechanisms to detect, investigate, and prosecute fraudulent activities. This article presents a comparative analysis of fraud-hunting institutions in seven countries: the United States, the United Kingdom, China, India, Germany, Nigeria, and Brazil. It explores the structure, powers, and operational strategies of government agencies and private auditors tasked with combating fraud, including the use of artificial intelligence, digital forensics, and inter-agency cooperation. The study draws on landmark investigations – such as the Enron scandal, LIBOR manipulation, the Wirecard collapse, and Brazil's Operation Car Wash – to highlight differences in institutional responses, transparency, and whistleblower protection. While advanced economies benefit from robust regulatory oversight and legal safeguards, emerging markets face challenges such as limited forensic capacity, political interference, and weaker protections for informants. Despite these differences, there is a global trend toward enhanced technological tools and cross-border enforcement collaboration. The analysis concludes that no single model guarantees success. Instead, effective anti-fraud efforts rely on a combination of legal authority, institutional independence, technological integration, and political will to act decisively against financial misconduct.

Keywords: financial fraud, anti-corruption, fraud investigation, regulatory agencies, forensic accounting, whistleblower protection, international cooperation, digital forensics

JEL Classification: D73, F53, G38, H83, K42, M42, O17

INTRODUCTION

In today's interconnected world, fraud has evolved from simple deception to sophisticated schemes that use technology to exploit vulnerabilities. Fraud has become a global problem that impacts economies, businesses, and individuals. From financial fraud and corporate abuse to cyber fraud and identity theft, criminals are constantly finding new ways to commit their financial crimes.

In response, countries have developed a variety of mechanisms to detect, investigate, and prevent fraudulent practices. These efforts are carried out by a growing network of fraud hunters–government agencies, regulators, forensic accountants, data professionals, and independent oversight bodies–who are dedicated to protecting institutional integrity and public trust. The role of fraud hunters is shaped by national legal systems, political contexts, technological capabilities, and levels of institutional transparency.

The study presents a comparative analysis of anti-fraud systems in six countries: the United States, the United Kingdom, China, India, Germany, Nigeria and Brazil. By examining the structure and effectiveness of the leading agencies in these countries and highlighting landmark cases, it is possible to trace both commonalities and differences in global anti-fraud strategies.

While countries such as the United States and the United Kingdom use interagency coordination and legal protection for whistleblowers, others such as China rely heavily on state oversight and centralized monitoring. Emerging economies such as India, Nigeria and Brazil face additional challenges related to judicial delays, political interference and limited forensic infrastructure, even as they solve some of the world's largest fraud cases.

This article examines how fraud hunters operate across countries, comparing institutional structures, investigative strategies, landmark cases, and enforcement challenges. It also highlights the growing role of artificial intelligence and cross-border cooperation in the fight against financial fraud. By examining these global approaches, we gain insight into the tools, tactics, and policies that define the modern era of fraud detection and enforcement.

LITERATURE REVIEW

The global fight against fraud has given rise to an increasingly diverse landscape of anti-fraud institutions and regulatory frameworks. Foundational theoretical models such as Cressey's (1953) Fraud Triangle and Wolfe and Hermanson's (2004) Fraud Diamond offer enduring insights into the psychological and structural conditions that enable fraudulent behaviour. These frameworks underpin much of the practical methodology applied by forensic experts and investigators worldwide (Albrecht et al., 2012).

Institutional responses to fraud differ significantly by region. In the United Kingdom, the emergence of the counter-fraud specialist and the evolution of organizations like the Serious Fraud Office (SFO) and Financial Conduct Authority (FCA) reflect a strategic shift toward specialized expertise and inter-agency collaboration (Button et al., 2007; Asher, 2025). Likewise, U.S. institutions such as the FBI, SEC, and IRS-CI demonstrate a multi-layered enforcement model backed by regulatory innovation, particularly in whistleblower protections and inter-agency cooperation (Dyck et al., 2010; Wells, 2018; Platt, 2024).

Emerging economies, however, present a more complex picture. In India, the work of CBI, SFIO, and RBI's Anti-Fraud Cell highlights the growing role of forensic accounting in corporate investigations (Bhasin, 2015; Deb, 2024). Yet, persistent challenges such as auditor resignations and delayed prosecutions remain (Banerjee, 2024). In Brazil, the landmark Lava Jato (Operation Car Wash) was a pivotal anti-corruption campaign, but critiques about legal inconsistency and politicization raise questions about the durability of reform (Cornelius, 2023). Nigeria's anti-fraud institutions, namely the EFCC and ICPC, have shown increased international cooperation in tackling cybercrime and high-level corruption (Williams, 2014; EFCC, 2025).

China presents a state-centric model where institutions like the CCDI, MPS, and CSRC operate with strong political backing. AI and surveillance technologies play a central role in fraud detection, though transparency and judicial independence remain limited (Yang et al., 2024; Xie et al., 2021). The study compiles a comprehensive database of Chinese officials convicted of corruption between 2012 and 2021, detailing their personal attributes and the amounts embezzled. The article aims to quantify the impact of the anti-corruption campaign on income inequality and political incentives by evaluating the extent to which corrupt gains propel officials into higher income brackets. In this context, the use of big data in identifying corruption has proven effective but also controversial.

Technological advancement is a recurring theme in global anti-fraud strategies. AI-based fraud detection systems, as reviewed by West and Bhattacharya (2016), are increasingly integrated into national investigative processes. Studies in digital fraud detection – such as UPI-based systems in India (Nazmoddin et al., 2024)–illustrate how machine learning is reshaping fraud surveillance. Blockchain technologies also offer new possibilities for transaction transparency and fraud prevention, particularly in supply chains and digital assets (Treiblmaier, 2018; Kou & Lu, 2025).

Whistleblower protection emerges as a critical component of fraud exposure. Dyck et al. (2010) and Platt (2024) emphasize that insiders are more likely than auditors or regulators to reveal corporate misconduct. Despite this, many countries lack robust legal frameworks to safeguard informants, limiting the potential of internal reporting systems.

Furthermore, comparative works such as Doig and Levi (2021) suggest that national strategies must balance legal enforcement with political realities and resource constraints. The article aims to provide a contemporary overview of the major issues in fraud and financial crime—such as prevention, public ethics, compliance, and law enforcement—within national strategic frameworks. They explore the persistent gap between high-level strategic intentions and their practical implementation «on the ground», highlighting issues of ownership, resourcing, and coordinated delivery across public and private sectors. In some cases, fraud is deeply entwined with governance challenges, especially in jurisdictions with weak rules of law or politicized institutions. Ultimately, the authors seek to inform and improve national strategic responses to fraud and financial crime by analysing trends, identifying implementation challenges, and proposing more joined-up and effective policy approaches.

DOI: 10.55643/ser.2.56.2025.606

Finally, the role of private sector auditors – such as PwC, Deloitte, KPMG, and EY–remains vital, though not without criticism. Failures in early fraud detection, such as in the Wirecard scandal, underscore the risks of audit capture and call for tighter regulation of auditing standards (Mock, 2021; Gottschalk & Gupta, 2024).

AIMS AND OBJECTIVES

This study aims to compare how different countries combat financial fraud by analyzing the structure, powers, and effectiveness of their key fraud-hunting institutions. It examines agencies in the United States, United Kingdom, China, India, Germany, Nigeria, and Brazil, focusing on their legal authority, use of technology, and collaboration in cross-border enforcement. The research also reviews major fraud cases to assess institutional performance and identifies areas for improvement, including legal reform, international cooperation, and whistleblower protection.

METHODS

This study adopts a qualitative, comparative approach to analyze how different countries combat financial fraud through institutional frameworks and enforcement strategies. It focuses on seven countries - the United States, United Kingdom, China, India, Germany, Nigeria, and Brazil – chosen for their diverse legal systems, economic contexts, and levels of institutional development. Data were drawn from official institutional websites, legal documents, investigative reports, and academic literature. The analysis centres on four core dimensions: institutional structure, legal authority, technological application, and enforcement effectiveness. These dimensions were examined through the lens of selected high-profile fraud cases, including the Enron scandal, LIBOR manipulation, the Ezubao Ponzi scheme, the PNB banking fraud, the Wirecard scandal, and Brazil's Operation Car Wash. These cases serve as illustrative examples to assess the capacity of national systems to detect, investigate, and prosecute fraud. Comparative tables were developed to synthesize key variables across jurisdictions, highlighting patterns of success, institutional limitations, and areas for improvement. Special attention was paid to the role of whistleblower protection, technological tools such as AI and forensic analytics, and the degree of international cooperation in fraud enforcement. This multi-dimensional approach enables a nuanced understanding of global anti-fraud efforts and provides a foundation for evaluating best practices.

RESULTS

1. Institutional mechanisms for detecting, investigating and prosecuting fraud

Fraud, in its many forms–ranging from Ponzi schemes and accounting fraud to cybercrime and state corruption–remains a persistent global threat. By examining the structure and impact of each country's primary investigative bodies and highlighting landmark cases, we can observe both convergence and divergence in global anti-fraud strategies.

The United States offers a robust and multi-layered framework for fraud detection, involving both civil and criminal authorities. The Federal Bureau of Investigation (FBI) leads criminal investigations into a range of frauds – including corporate, healthcare, and cyber-related crimes – while the Securities and Exchange Commission (SEC) regulates financial markets, focusing on insider trading, securities fraud, and market manipulation. Additionally, the Internal Revenue Service Criminal Investigation (IRS-CI) investigates tax evasion and money laundering, often partnering with other federal agencies. The Consumer Financial Protection Bureau (CFPB) complements these efforts by focusing on consumer-facing fraud in the banking and lending sectors. In the private sector, firms like Kroll, PwC, and Deloitte carry out forensic audits, often uncovering fraud that feeds into official investigations.

One of the most infamous frauds in U.S. history was the Bernie Madoff Ponzi scheme, which defrauded investors of an estimated USD 65 billion. The investigation, led by the SEC and the FBI, revealed systemic failures in regulatory oversight and resulted in Madoff's conviction and a 150-year prison sentence.

The United Kingdom also employs a multifaceted approach, characterized by specialized agencies and strong regulatory mechanisms. The Serious Fraud Office (SFO) prosecutes high-level financial crimes, such as bribery and corruption, and has the authority to seize assets and compel testimony. Complementing the SFO, the National Crime Agency (NCA) tackles organized financial crime and cross-border laundering, while Action Fraud provides a public-facing platform for victims to report scams. The Financial Conduct Authority (FCA) supervises financial institutions and ensures compliance with ethical and regulatory standards.

The LIBOR manipulation scandal stands out as a pivotal case in the UK, exposing how major banks, including Barclays, manipulated global interest rates for profit. The SFO's investigation led to criminal charges, substantial fines, and a broader reform of financial benchmarks, revealing the systemic reach of market abuse and the importance of vigilant oversight.

In China, fraud investigations are tightly integrated into state-led governance, combining political oversight with cutting-edge technology. The Central Commission for Discipline Inspection (CCDI) plays a central role in investigating corruption within the Communist Party and state apparatus. Meanwhile, the Ministry of Public Security (MPS) handles financial crimes and cyber fraud, with support from the China Banking and Insurance Regulatory Commission (CBIRC), which oversees the integrity of financial institutions. Notably, China employs AI and big data analytics for real-time monitoring of financial transactions, making it one of the most technologically advanced fraud detection systems globally.

A key example of fraud detection in action was the Ezubao Ponzi scheme, in which nearly one million investors were duped into placing funds in fake online investment products, totalling USD 7.6 billion. Authorities swiftly dismantled the scheme and sentenced executives to life imprisonment, underscoring the state's zero-tolerance approach–albeit within a tightly controlled political and media environment.

India's fraud-hunting system operates primarily through government agencies. The Central Bureau of Investigation (CBI) leads criminal probes into large-scale fraud and corruption. The Serious Fraud Investigation Office (SFIO), established under the Companies Act, focuses on complex corporate fraud, while the Reserve Bank of India (RBI) maintains an anti-fraud cell that monitors banking institutions for irregularities and signs of internal collusion.

A prominent case illustrating systemic vulnerabilities is the Punjab National Bank (PNB) fraud, where jeweler Nirav Modi orchestrated a USD 2 billion scam using fake letters of credit to obtain loans. The CBI and SFIO jointly investigated the case, resulting in high-profile arrests and extradition efforts, and spurred regulatory reforms in Indian banking practices.

Germany's fraud detection architecture is known for its regulatory precision. The Federal Financial Supervisory Authority (BaFin) is responsible for oversight of banks, insurers, and financial markets. The Federal Criminal Police Office (BKA) leads criminal investigations into white-collar crimes, and private auditing firms – such as KPMG, Deloitte, and EY – play an integral role in fraud detection through forensic audits.

However, the Wirecard scandal revealed significant blind spots in Germany's oversight system. The fintech company falsely claimed to hold EUR 1.9 billion in overseas accounts, misleading regulators and investors. Despite red flags raised by journalists and whistleblowers, BaFin failed to act decisively, leading to public outcry and scrutiny of Germany's financial regulatory culture. The subsequent arrest of Wirecard's CEO marked a turning point in calls for reform.

Nigeria's approach to fraud prevention is focused on anti-corruption and cyber fraud enforcement. The Economic and Financial Crimes Commission (EFCC) is the country's primary anti-fraud agency, targeting scams, email fraud, and money laundering. The Independent Corrupt Practices Commission (ICPC) handles fraud and ethical misconduct in public office.

A landmark case involved Ramon "Hushpuppi" Abbas, a social media influencer who orchestrated cyber scams targeting individuals and companies across continents. His arrest, conducted in collaboration with the FBI, highlighted Nigeria's evolving role in addressing digital fraud and demonstrated the importance of transnational investigative partnerships.

Brazil has gained international recognition for its efforts to investigate entrenched corruption through the Federal Police and the Public Ministry (MPF). These bodies have been central to Operation Car Wash (Lava Jato), a sprawling investigation that uncovered widespread corruption in state oil company Petrobras. Executives and politicians across Latin America were implicated in bribe-taking and contract rigging, totalling billions of dollars.

The investigation led to over 200 arrests, including former president Luiz Inácio Lula da Silva, and marked one of the largest anti-corruption drives in history. Despite its initial success, Lava Jato faced setbacks amid political backlash, raising concerns about the sustainability of such operations in highly polarized environments.

2. Comparative Analysis of Fraud-Hunting Bodies Across the World

Fraud-hunting bodies worldwide differ in their structure, scope, and approach. While some focus on corporate fraud, others deal primarily with corruption, cyber fraud, or financial misconduct. This comparative analysis highlights key differences and similarities in mandates, investigative powers, methods, and effectiveness across various institutions.

Table 1 presents a comparison that looks at the institutional structure and core responsibilities of anti-fraud authorities in seven countries, highlighting how different systems approach the common problem of financial fraud.

DOI: 10.55643/ser.2.56.2025.606

Table 1. Structural Comparison: Government, independent and private Bodies.

Country	Fraud-Hunting Body	Type of Institution	Primary Focus
The U.S.	FBI, SEC, IRS-CI	Government agencies	Corporate fraud, securities fraud, tax evasion
U.K.	SFO, FCA, NCA	Government agencies with independent oversight	Financial crime, corporate fraud, bribery
China	CCDI, MPS, CSRC	Government agencies, some under Communist Party control	Corruption, banking fraud, cyber fraud
India	CBI, SFIO, RBI Anti-Fraud Cell	Government agencies	Banking fraud, corporate fraud, tax evasion
Germany	BaFin, BKA, Private Auditors	Government agencies and private forensic firms	Financial fraud, regulatory breaches
Nigeria	EFCC, ICPC	Government anti-corruption agencies	Corruption, cyber fraud, money laundering
Brazil	Federal Police, MPF (Public Ministry)	Law enforcement and judiciary collaboration	Bribery, corporate corruption, money laundering

The comparative analysis reveals that while all examined countries recognize the seriousness of financial fraud, their institutional responses are shaped by distinct political, legal, and economic contexts. The United States and the United Kingdom rely on multi-agency frameworks with strong regulatory oversight and legal protections. In contrast, countries like China adopt centralized, state-driven models with heavy technological surveillance. Meanwhile, emerging economies such as India, Nigeria, and Brazil confront resource constraints but have demonstrated growing capacity through high-profile anti-corruption campaigns. These structural differences underscore the importance of tailoring anti-fraud strategies to local governance models while promoting international cooperation in combating cross-border fraud.

The effectiveness of anti-fraud agencies in different countries depends not only on their institutional presence but also on the powers granted to them by law. Investigative powers, such as the ability to arrest, prosecute, seize assets or impose regulatory sanctions, vary significantly between national authorities. Table 2 compares the legal powers and enforcement methods of leading anti-fraud agencies from the United States, the United Kingdom, China, India, Germany, Nigeria and Brazil. It highlights how each agency carries out its mandate, the tools it uses and the scope of its jurisdiction, particularly in the context of transnational financial crime.

Table 2. Investigative Powers: Authority and Enforcement Mechanisms.

Body	Powers	Legal Authority	Methods Used
FBI (U.S.)	Federal investigation, arrests, surveillance	National & International (Interpol cooperation)	Cyber forensics, undercover operations, subpoenas
SEC (U.S.)	Civil enforcement, fines, bans on companies	National, collaborates with DOJ	Audits, whistleblower programs, forensic accounting
SFO (U.K.)	Criminal prosecution, asset seizures	National	Wiretaps, forensic accounting, intelligence sharing
CCDI (China)	Party discipline, arrests of officials	National, party-controlled	Surveillance, AI-driven financial tracking
CBI (India)	Criminal investigations, arrests	National, court-driven prosecutions	Financial audits, corporate probes
BaFin (Germany)	Regulatory oversight, fines, bans	National, European banking laws	Risk analysis, forensic audits
EFCC (Nigeria)	Criminal investigations, cybercrime tracking	National & International (Interpol collaboration)	Digital forensics, sting operations
Federal Police (Brazil)	Criminal prosecution, asset freezing	National, works with the judiciary	Wiretaps, forensic financial tracking

The analysis shows that while countries like the United States and the United Kingdom lead in technological deployment and legal safeguards for whistleblowers, others – such as China, India, and Nigeria – face challenges related to transparency and whistleblower risk. Inter-agency collaboration is widespread, but the effectiveness of these partnerships often depends on broader institutional independence and access to secure data systems. Although technological progress has enhanced fraud detection capabilities, a balanced approach that combines digital tools with strong human oversight and legal protections remains essential for sustainable anti-fraud enforcement.

In the digital age, the fight against financial fraud increasingly relies on technological innovation and coordinated intelligence sharing. Fraud-hunting bodies around the world are adopting tools like artificial intelligence, big data analytics, and forensic technologies to detect irregularities and respond quickly to complex schemes. At the same time, collaboration between domestic and international agencies has become vital for tracking cross-border operations. Yet, the effectiveness of these systems is also shaped by how well countries protect whistleblowers–individuals who often play a pivotal role in exposing fraud from within (Table 3).

Table 3. Investigative Methods: Technology and Intelligence Sharing.

Country	Use of AI/Tech	Collaboration with Other Agencies	Whistleblower Protection
The U.S.	Advanced AI, big data fraud detection	FBI, SEC, IRS, Interpol	Strong (Dodd-Frank Act protects whistleblowers)
U.K.	Data analytics for financial fraud tracking	SFO, FCA, Action Fraud	Moderate (Public Interest Disclosure Act)
China	AI-driven financial monitoring, facial recognition	MPS, CSRC, CCDI	Weak (Whistleblowers face political risks)
India	Banking fraud detection via AI, forensic accounting	CBI, SFIO, RBI	Weak (Whistleblowers lack full legal protection)
Germany	Predictive risk analysis in financial markets	BaFin, BKA, European regulators	Moderate (Whistleblower Protection Act)
Nigeria	Digital forensics, blockchain tracking	EFCC, ICPC, Interpol	Weak (Whistleblower's face intimidation)
Brazil	Financial intelligence, forensic accounting	Federal Police, MPF, Lava Jato	Moderate (Limited protection in corruption cases)

The comparative overview highlights both progress and disparity. Countries like the United States and the United Kingdom have integrated advanced technology into fraud detection and maintain moderate to strong legal frameworks for whistleblower protection. Others, such as China, India, and Nigeria, employ sophisticated tools but lack robust safeguards for those who report misconduct, limiting the overall effectiveness of their systems. While intelligence-sharing networks are improving globally, the balance between high-tech solutions and legal protections remains a key factor in successful fraud prevention and enforcement.

Assessing the effectiveness of fraud-hunting bodies requires looking beyond their mandates and powers to examine real-world outcomes. High-profile fraud cases provide insight into how well national systems respond when faced with major financial deception. By analyzing landmark investigations across several countries, this section evaluates not only the scale of fraud uncovered but also the legal, institutional, and political consequences that followed. These cases reveal the capacity of institutions to prosecute offenders, recover assets, and implement reforms (Table 4).

Table 4. Effectiveness & Success in Major Investigations.

Country	Notable Case	Fraud Amount	Outcome
The U.S.	Enron (2001)	USD 74 billion	CEO jailed, SOX Act introduced
U.K.	LIBOR Scandal (2012)	Global market manipulation	Bankers jailed, regulatory reforms
China	Ezubao Ponzi Scheme (2016)	USD 7.6 billion	Executives jailed, AI fraud tracking improved
India	PNB Bank Fraud (2018)	USD 2 billion	Fugitive Nirav Modi arrested
Germany	Wirecard Scandal (2020)	EUR 1.9 billion	CEO jailed, BaFin criticized
Nigeria	Hushpuppi Cyber Fraud (2020)	USD 300 million	Arrested, sentenced in U.S.
Brazil	Operation Car Wash (2014)	USD 788 million	Over 200 arrests, political impact

The outcomes of major investigations demonstrate varying levels of success in combating fraud. In countries like the United States and the United Kingdom, fraud cases have led to significant legal reforms and criminal convictions, reinforcing institutional credibility. China and Germany responded decisively to corporate scandals but also faced criticism regarding transparency and regulatory oversight. In emerging economies like India, Nigeria, and Brazil, investigations exposed large-scale corruption and cybercrime, though enforcement outcomes often depended on international cooperation or political

DOI: 10.55643/ser.2.56.2025.606

momentum. Overall, these cases show that effective fraud enforcement hinges not only on detection but on the political will and legal capacity to act decisively.

DISCUSSION

The findings of this study reveal significant variation in how countries organize and empower their fraud-hunting institutions. Despite a shared recognition of the growing threat posed by financial fraud, national approaches differ according to legal traditions, political environments, economic resources, and technological capacities.

Countries such as the United States and the United Kingdom demonstrate relatively mature and institutionalized anti-fraud systems. These systems are characterized by inter-agency collaboration, strong legal mandates, and protections for whistleblowers. The integration of civil and criminal authorities, as seen in the cooperation between the FBI, SEC, and IRS-CI in the U.S., enhances investigative reach and improves prosecution outcomes. Similarly, the UK's Serious Fraud Office and Financial Conduct Authority provide a strong framework for prosecuting high-level financial crimes, as illustrated by the LIBOR scandal.

In contrast, China relies heavily on centralized and state-led enforcement, combining political oversight with sophisticated technological surveillance. Institutions like the CCDI and MPS play dual roles in law enforcement and political control, with AI and big data analytics used extensively in fraud detection. However, concerns remain regarding transparency, due process, and the treatment of whistleblowers. Although such systems can be highly efficient in dismantling fraud schemes – as seen in the Ezubao case – they may lack accountability and external oversight.

Emerging economies such as India, Nigeria, and Brazil face structural challenges in fraud enforcement. These include limited forensic capacity, judicial inefficiencies, and political interference. Nonetheless, high-profile investigations – such as India's PNB banking scandal, Nigeria's prosecution of cybercriminals like Hushpuppi, and Brazil's Operation Car Wash – highlight increasing efforts to address large-scale fraud and corruption. These cases demonstrate the growing importance of international cooperation and transnational enforcement mechanisms, particularly in addressing cybercrime and cross-border financial flows.

The role of technology is a common theme across all jurisdictions. Countries are increasingly investing in AI-driven fraud detection, data analytics, and digital forensics. While the United States and Germany apply such tools within well-established legal and regulatory frameworks, other countries implement them in more politically influenced environments. The use of technology, while enhancing detection capabilities, raises new questions about privacy, surveillance, and the potential for misuse – especially where legal safeguards are weak.

Another critical issue is whistleblower protection. The United States stands out for offering legal and financial incentives for whistleblowers, which has contributed to the early detection of major frauds. In contrast, countries like China, Nigeria, and India lack robust protections, which discourages insiders from coming forward and limits institutional transparency.

Overall, the comparative analysis suggests that there is no one-size-fits-all model for fraud enforcement. While institutional design matters, the political will to enforce laws, protect whistleblowers, and invest in investigative capacity is equally crucial. Moreover, as financial crime becomes increasingly borderless, international coordination and harmonization of anti-fraud standards will be essential to long-term success.

CONCLUSIONS

This research has shown that while financial fraud is a global problem, the structures and strategies used to fight it vary widely across countries. Fraud-hunting bodies operate within different legal, political, and technological contexts, influencing their effectiveness and approach. Developed countries like the United States and the United Kingdom benefit from strong regulatory frameworks, institutional independence, and inter-agency coordination. Their use of advanced technologies and legal protections for whistleblowers further strengthens enforcement efforts.

In contrast, countries such as China rely on centralized control and surveillance-driven models, which can be efficient but raise concerns about transparency and accountability. Emerging economies like India, Nigeria, and Brazil face challenges such as limited resources and political interference but have made notable progress through high-profile investigations and growing international cooperation.

Technology, especially artificial intelligence and forensic analytics, plays an increasingly important role in modern fraud detection. However, its effectiveness depends on how well it is integrated into legal systems that uphold due process and transparency. Additionally, whistleblower protection remains a critical factor in uncovering fraud and must be strengthened, particularly in countries where risks for informants remain high.

Ultimately, the fight against fraud requires a balanced approach that combines strong institutions, modern technology, legal safeguards, and global collaboration. As financial crimes continue to evolve, so too must the systems designed to detect and prevent them. Future research should focus on such systems that will help detect and prevent financial crimes.

ADDITIONAL INFORMATION

FUNDING

The Author received no funding for this research.

CONFLICT OF INTEREST

The Author declares that there is no conflict of interest.

REFERENCES

1. Abia, W. A., Haughey, S. A., Radhika, R., Taty, B. P., Russell, H., Carey, M., Maestroni, B. M., Petchkongkaew, A., Elliott, C. T., & Williams, P. N. (2025). Africa, an Emerging Exporter of Turmeric: Combating Fraud with Rapid Detection Systems. *Foods*, *14*(9), 1590. https://doi.org/10.3390/foods14091590
2. Albrecht, W. S., Albrecht, C. O., Albrecht, C. C., & Zimbelman, M. F. (2012). *Fraud examination* (4th ed.). Cengage Learning.
3. Asher, J. (2025). *Fraud Markers, De-banking, and Financial Crime: A Legal Analysis of Counter-fraud Practices in the UK and Beyond*. Taylor & Francis. https://doi.org/10.4324/9781003588542
4. Banerjee, R. (2024). Who Cheats and How: Scams, Frauds and the Dark Side of the Corporate World. Penguin Random House India Private Limited.
5. Bhasin, M. L. (2015). Forensic accounting and fraud: An empirical study of India. *International Journal of Management Sciences and Business Research*, *4*(10), 36-45. https://doi.org/10.4236/ojacct.2016.54007
6. Button, M., Johnston, L., Frimpong, K., & Smith, G. (2007). New directions in policing fraud: The emergence of the counter fraud specialist in the United Kingdom. *International journal of the sociology of law*, *35*(4), 192-208. https://doi.org/10.1016/j.ijsl.2007.06.002
7. Central Bureau of Investigation (CBI). (2025). Home. https://cbi.gov.in
8. Central Commission for Discipline Inspection (CCDI). (2025). Home. http://www.ccdi.gov.cn
9. China Securities Regulatory Commission (CSRC). (2025). Home. http://www.csrc.gov.cn
10. Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*(4), 588–608. https://doi.org/10.2307/2094589
11. Cornelius, E. (2023). Discursive mismatch and globalization by stealth: the fight against corruption in the Brazilian legal field. *Law & Society Review*, *57*(3), 340-363. https://doi.org/10.1111/lasr.12664
12. Cressey, D. R. (1953). *Other people's money: A study in the social psychology of embezzlement*. Free Press. https://psycnet.apa.org/record/1954-06293-000
13. Deb, R. (2024). Fraud Prevention and Auditors' Resignation: Indian Evidence. *Metamorphosis, 24*(1), 21-30. https://doi.org/10.1177/09726225241261773
14. Deloitte. (2025). Home. https://www.deloitte.com/ua/uk.html
15. Doig, A., & Levi, M. (2021). Frauds and financial crimes: national strategic. *Frauds and Financial Crimes: Trends, Strategic Responses, and Implementation Issues in England and Wales*. https://doi.org/10.4324/9781003178989
16. Dr. Nazmoddin, M.D., Swetha, M., Yashwanthi, G., & Divyasree, Y. (2024). UPI Fraud Detection Using Machine Learning. *Journal of Computational Analysis and Applications (JoCAAA), 33*(06), 1704–1707. https://eudoxuspress.com/index.php/pub/article/view/2503
17. Dyck, A., Morse, A., & Zingales, L. (2010). Who blows the whistle on corporate fraud? *The Journal of Finance*, *65*(6), 2213–2253. https://doi.org/10.1111/j.1540-6261.2010.01614.x
18. Economic and Financial Crimes Commission (EFCC). (2025). Home. https://www.efcc.gov.ng
19. Ernst & Young (EY). (2025). Home. https://www.ey.com
20. Federal Bureau of Investigation (FBI). (2025). Home. https://www.fbi.gov
21. Federal Criminal Police Office (BKA). (2025). Home. https://www.bka.de
22. Federal Financial Supervisory Authority (BaFin). (2025). Home. https://www.bafin.de

DOI: 10.55643/ser.2.56.2025.606

23. Federal Police (Polícia Federal). (2025). Home. https://www.gov.br/pf

24. Financial Conduct Authority (FCA). (2025). Home. https://www.fca.org.uk

25. Gottschalk, P. (2010). *Policing white-collar crime: Characteristics of white-collar criminals*. CRC Press. https://doi.org/10.1201/b16232

26. Gottschalk, P., & Gupta, C.M. (2024). RETRACTED CHAPTER: Stock Manipulation and Accounting Fraud. In: RETRACTED BOOK: Review of Corporate Internal Fraud Investigations. Springer, Cham. https://doi.org/10.1007/978-3-031-60758-5_3

27. Independent Corrupt Practices Commission (ICPC). (2025). Home. https://icpc.gov.ng

28. Internal Revenue Service – Criminal Investigation (IRS-CI). (n.d.). Criminal Investigation Division. https://www.irs.gov/compliance/criminal-investigation

29. Kou, G., & Lu, Y. (2025). FinTech: a literature review of emerging financial technologies and applications. *Financ Innov, 11*(1). https://doi.org/10.1186/s40854-024-00668-6

30. KPMG. (2025). Home. https://home.kpmg

31. Ministério Público Federal (MPF). (2025). Home. https://www.mpf.mp.br

32. Ministry of Public Security (MPS). (2025). Home. http://www.mps.gov.cn

33. Mock, S. (2021). Wirecard and European Company and Financial Law. *European Company and Financial Law Review, De Gruyter, 18*(4), 519-554. https://doi.org/10.1515/ecfr-2021-0024

34. National Crime Agency (NCA). (2025). Home. https://www.nationalcrimeagency.gov.uk

35. Platt, A. I. (2024, March 1). The Shortseller Enrichment Commission? Whistleblowers, Activist Short Sellers, and the New Privatization of Public Enforcement. *Washington Law Review, 99*. https://ssrn.com/abstract=4744972

36. PwC (PricewaterhouseCoopers). (2025). Home. https://www.pwc.com

37. Reserve Bank of India (RBI) – Anti-Fraud Cell. (2025). Home. https://www.rbi.org.in

38. Serious Fraud Investigation Office (SFIO). (2025). Home. https://sfio.nic.in

39. Serious Fraud Office (SFO). (2025). Home. https://www.sfo.gov.uk

40. Treiblmaier, H. (2018). The impact of blockchain on the supply chain: A theory-based research framework and a call for action. *Supply Chain Management: An International Journal*, *23*(6), 545–559. https://doi.org/10.1108/SCM-01-2018-0029

41. U.S. Securities and Exchange Commission (SEC). (2025). Home. https://www.sec.gov

42. Wells, J. T. (2018). *International Fraud Handbook*. John Wiley & Sons. https://doi.org/10.1002/9781119448709

43. West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. *Computers and Security*, *57*, 47-66. https://doi.org/10.1016/j.cose.2015.09.005

44. Williams, P. (2014). Nigerian criminal organizations. In *The Oxford handbook of organized crime* (pp. 254-269). Oxford: Oxford University Press. https://shorturl.at/GtehG

45. Wolfe, D., & Hermanson, D. R. (2004). The Fraud Diamond: Considering Four Elements of Fraud. *The CPA Journal, 74*, 38-42. https://doi.org/10.1016/S1361-3723(04)00065-X

46. Yang, L., Milanovic, B., & Lin, Y. (2024). Anti-corruption campaign in China: An empirical investigation. *European Journal of Political Economy*, *85*, 102559. https://doi.org/10.1016/j.ejpoleco.2024.102559

Мігус І.

МИСЛИВЦІ НА ШАХРАЙСТВО У СВІТІ: БОРОТЬБА З ОБМАНОМ У РІЗНИХ КРАЇНАХ

У відповідь на зростання кількості складних фінансових злочинів країни світу розробили різні антикорупційні та антишахрайські системи, адаптовані до їхніх правових, політичних і технологічних реалій. У статті представлено порівняльний аналіз інституцій боротьби з шахрайством у США, Великій Британії, Китаї, Індії, Німеччині, Нігерії та Бразилії. Розглянуто органи державного контролю та приватних аудиторів, які займаються виявленням, розслідуванням і переслідуванням випадків шахрайства із застосуванням таких інструментів, як штучний інтелект, цифрова криміналістика та міжвідомча співпраця. На основі аналізу резонансних справ – таких як скандали з Enron, маніпуляції LIBOR і операція «Автомийка» – автори висвітлюють відмінності в повноваженнях, захисті викривачів та ефективності систем. Розвинені країни демонструють високий рівень регулювання та інституційної незалежності, водночас країни, що розвиваються, стикаються з проблемами політичного тиску та обмеженими ресурсами. Особливу увагу приділено ролі міжнародної співпраці в боротьбі з транскордонним шахрайством. У результаті дослідження зроблено висновок, що ефективність боротьби з шахрайством залежить не лише від технологій, а й від законодавчих гарантій, прозорості та політичної волі.

Ключові слова: фінансове шахрайство, антикорупція, розслідування шахрайства, регуляторні органи, судово-бухгалтерська експертиза, захист викривачів, міжнародна співпраця, цифрова криміналістика

JEL Класифікація: D73, F53, G38, H83, K42, M42, O17