World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Fraud Hexagon in the COVID-19 Environment: An Analytical Examination of Causes, Mechanisms, and Impacts: A Review

Mudzamir Mohamed *

Senior Lecturer, Tunku Puteri Intan Safinas School of Accountancy. Universiti Utara Malaysia, Sintok, Kedah, Malaysia.

World Journal of Advanced Research and Reviews, 2025, 28(03), 862-869

Publication history: Received on 31 October 2025; revised on 09 December 2025; accepted on 11 December 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.28.3.4130

Abstract

The COVID-19 pandemic created unprecedented conditions that intensified and diversified fraudulent activities across global systems. Economic disruption, institutional strain, rapid digital transformation, and heightened public uncertainty collectively expanded opportunities for deception and exploitation. This paper examines fraud in the pandemic environment through the lenses of the Fraud Triangle and Fraud Hexagon, highlighting how pressure, opportunity, rationalization, capability, collusion, and arrogance converged to fuel misconduct. Key manifestations included health and medical fraud, government relief and subsidy abuse, cyber scams, investment schemes, insurance fraud, and corporate reporting manipulation. The analysis underscores how crisis governance—marked by rapid relief distribution, fragmented data systems, limited oversight, and digital inequality—created systemic vulnerabilities. Findings reveal that pandemic-driven fraud eroded public trust, entrenched cybercrime infrastructures, and imposed lasting regulatory burdens. The study concludes that future crisis responses must balance speed with resilience, integrating digital identity systems, real-time analytics, and adaptive fraud-prevention strategies to safeguard institutions and societies against exploitation in times of emergency.

Keywords: Healthcare fraud; White collar fraud; Fraud Hexagon; Pandemic

1 Introduction

The COVID-19 pandemic did not only produce a global health crisis; it triggered profound economic, social, and institutional disruption that created fertile ground for fraudulent activities. As governments rushed to provide economic support, organizations rapidly transitioned to remote operations, and individuals adapted to digital services, vulnerabilities emerged across financial, technological, and administrative systems. Fraud as a deliberate deception for personal or financial gain which thrived in this environment (1). The pandemic became a catalyst for the intensification, diversification, and sophistication of fraud schemes worldwide.

Beyond its immediate health and economic consequences, the pandemic exposed the fragility of governance structures and the adaptability of fraudulent actors. Crises historically magnify fraud risks, but COVID-19 was distinctive in its global reach, speed of disruption, and reliance on digital infrastructures. The convergence of emergency funding, weakened institutional oversight, and widespread psychological vulnerability created a “perfect storm” in which fraud could flourish (1) (7). This environment blurred traditional boundaries between white-collar crime, cybercrime, and opportunistic deception, revealing how fraud evolves dynamically in response to systemic shocks.

This review examines the relationship between fraud and the COVID-19 environment by exploring how pandemic-related pressures, digital shifts, weakened controls, emergency funding, and heightened uncertainty collectively increased fraud risks (7). Using fraud theory frameworks such as the Fraud Triangle and Fraud Hexagon, supported by evidence from academic studies and global enforcement data, the essay provides a comprehensive analysis of why fraud

* Corresponding author: Mudzamir Mohamed

proliferated during COVID-19, what forms it took, and what structural weaknesses the pandemic revealed. In doing so, it situates pandemic-driven fraud within broader debates on crisis governance, resilience, and institutional trust. The discussion concludes with implications for designing adaptive fraud-prevention strategies, strengthening digital accountability, and building governance systems capable of withstanding future global emergencies (8).

2 The COVID-19 Environment as a Catalyst for Fraud

The COVID-19 environment can be understood as an intersection of crisis dynamics: economic stress, rapid digital transformation, institutional strain, and heightened public fear (2). These conditions altered both individual and organizational behaviours, weakened oversight mechanisms, and expanded opportunities for exploitation. Fraud risk increased not because human nature changed, but because the systemic environment became more permissive and chaotic.

2.1 Economic Shock and Financial Pressure

The economic consequences of lockdowns, business closures, and job losses heightened financial pressure on individuals and corporations. Millions faced income reduction or unemployment. Research on criminology (7) suggests that financial stress acts as a significant driver of fraudulent behaviour, especially in environments where access to legitimate income becomes uncertain. For businesses, the sudden decline in sales, supply-chain disruptions, and liquidity shortages created strong incentives to manipulate financial statements, exaggerate losses to obtain support, or engage in fraudulent loan applications.

2.2 Institutional Strain and Reduced Oversight

Governments and regulatory bodies were overwhelmed by the urgency and scale of pandemic response. Emergency funds, economic stimulus packages, and relief programs were implemented rapidly, often bypassing normal verification procedures. Many systems were designed for speed rather than security. Public agencies (7) faced workforce shortages, remote operations, and procedural disruptions that weakened monitoring and enforcement capabilities. This institutional strain created loopholes for opportunistic fraudsters and sophisticated criminal networks alike.

2.3 Widespread Migration to Digital Platforms

COVID-19 accelerated digital transformation at an unprecedented pace. Consumers shifted to e-commerce, online banking, telemedicine, and virtual communication. Businesses adopted remote-work arrangements and cloud-based systems. While these transitions enabled continuity, they also exposed populations to unfamiliar digital risks and created new attack surfaces for cybercriminals (2). Those with limited digital literacy—elderly populations, newly online users, and small businesses—became particularly vulnerable to phishing, identity theft, and online investment fraud.

2.4 Public Uncertainty and Psychological Vulnerability

Fear, confusion, and misinformation surrounded the early stages of the pandemic. Fraudsters exploited this psychological environment by promoting fake cures, counterfeit test kits, fraudulent vaccination appointments, and deceptive health products. The sense of urgency and panic lowered people's natural scepticism, making them more susceptible to scams. Social engineering attacks became more effective in a context where reliable information was scarce and people sought quick solutions (7).

3 Fraud Through the Lens of the Fraud Triangle and Fraud Hexagon

Figure 1 Fraud Hexagon elements (3)(4)(5)(6)

The COVID-19 pandemic created a unique confluence of pressures, vulnerabilities, and behavioural shifts that catalysed fraudulent activity across sectors. Drawing on an expanded fraud hexagon framework, this section explores six interrelated dimensions—pressure, opportunity, rationalization, capability, collusion, and arrogance—that shaped the fraud landscape during the crisis (3) (4)(5).

3.1 Pressure (Incentive)

The pandemic-induced economic shock significantly heightened financial strain for individuals and organizations. Widespread income loss, business disruption, and market volatility intensified incentives to engage in fraudulent behavior. Individuals, facing existential financial insecurity, often rationalized fraudulent claims for government aid as a necessary survival strategy. Concurrently, corporate actors that is particularly those under investor scrutiny was faced mounting pressure to maintain performance metrics, leading to manipulation of financial statements and opportunistic exploitation of subsidy programs (4). This pressure dimension aligns with classical fraud theory; wherein economic incentives act as a primary driver of deviant behaviours under crisis conditions.

3.2 Opportunity

The rapid shift to remote operations and emergency relief mechanisms weakened traditional control environments. Opportunities for fraud proliferated due to (3):

- Diminished internal controls under remote work arrangements
- Overwhelmed and understaffed government agencies
- Expedited disbursement protocols with reduced verification
- Accelerated digitalisation without commensurate cybersecurity investment
- Increased reliance on online transactions and digital interfaces

These systemic vulnerabilities created permissive environments for fraud, where detection probabilities were markedly reduced. The convergence of technological expansion and oversight fatigue rendered many institutions ill-equipped to monitor and mitigate emerging threats (5).

3.3 Rationalization

Crisis conditions reshaped moral reasoning and ethical boundaries. Individuals and entities engaged in cognitive reframing to justify fraudulent acts, often invoking narratives such as(4):

- “Everyone is struggling; I deserve this support.”

- "The government has ample resources; this won't hurt anyone."
- "Extraordinary times require bending the rules."

Such rationalizations facilitated the erosion of normative constraints, allowing perpetrators to maintain a self-perception of legitimacy while engaging in misconduct. This behavioural dimension (3) underscores the psychological elasticity of ethical standards under duress.

3.4 Capability

Pandemic-era fraud increasingly demanded technical sophistication. Perpetrators leveraged digital fluency, system knowledge, and procedural insight to exploit vulnerabilities (1). Cybercriminals rapidly adapted to pandemic themes, deploying targeted phishing campaigns, spoofed relief portals, and malware tailored to remote-work infrastructures. Organized fraud networks demonstrated operational agility, automating large-scale claims across multiple jurisdictions. The capability dimension reflects the growing intersection between fraud and cybercrime, necessitating enhanced digital forensic capacity within regulatory frameworks (7).

3.5 Collusion

Fraud schemes during COVID-19 frequently involved coordinated efforts among multiple actors (5). Examples include:

- Identity brokers trafficking stolen credentials
- Insiders manipulating internal systems to approve false claims
- Transnational networks orchestrating online scams
- Suppliers conspiring to inflate prices of personal protective equipment (ppe)

Collusion amplified both the scale and complexity of fraudulent operations, challenging traditional detection models that focus on individual deviance. The collaborative nature of pandemic fraud underscores the need for inter-agency intelligence sharing and cross-sectoral vigilance.

3.6 Arrogance

A subset of perpetrators exhibited a sense of impunity, believing the crisis context shielded them from scrutiny. This was particularly evident in financial reporting and procurement fraud, where actors assumed regulatory bodies were too distracted or under-resourced to enforce compliance (3)(4). Such arrogance was rooted in perceived invulnerability that also fuelled high-risk behavior and strategic exploitation of oversight gaps. This dimension reflects a psychological disposition that thrives in environments of institutional fatigue and regulatory ambiguity.

4 Types of Fraud that Emerged or Intensified During COVID-19

The COVID-19 pandemic did not merely amplify the volume of fraudulent activity; it catalysed a diversification of fraud typologies across sectors. The crisis environment—characterized by urgency, digital acceleration, and regulatory disruption—enabled novel schemes and intensified existing ones. The following subsections delineate major categories of fraud that proliferated during the pandemic, each reflecting distinct vulnerabilities within governance, economic, and technological systems.

4.1 Health and Medical Fraud

The global scarcity of medical supplies, coupled with heightened public anxiety, created fertile ground for health-related fraud. Criminal actors exploited supply-chain disruptions and regulatory gaps to distribute substandard or fictitious products (9) (10). Common manifestations included:

- Counterfeit N95 masks and personal protective equipment (PPE)
- Falsified COVID-19 test kits and vaccination certificates
- Unauthorized "cures," herbal remedies, and unverified treatments
- Fraudulent scheduling of vaccination appointments

These schemes not only undermined public health efforts but also eroded trust in medical institutions and regulatory authorities. The transnational nature of medical fraud during the pandemic underscores the need for coordinated oversight and product authentication mechanisms.

4.2 Government Relief and Subsidy Fraud

Emergency fiscal interventions—such as stimulus payments, wage subsidies, business continuity loans, and unemployment benefits—became prime targets for exploitation (7)(11). Fraudulent claims often involved:

- Misrepresentation or exaggeration of financial distress
- Duplication of applications across programs
- Use of stolen or synthetic identities
- False declarations regarding business operations or workforce impact

The sheer scale and urgency of relief disbursements, often executed with relaxed verification protocols, rendered these programs vulnerable. Empirical data from multiple jurisdictions (7) revealed billions in misappropriated funds, highlighting the tension between rapid economic support and fiscal accountability.

4.3 Cyber Fraud and Online Scams

The pandemic accelerated digital migration, exposing individuals and institutions to heightened cyber risk (5)(6). Fraudulent activities in the digital domain included:

- Phishing campaigns impersonating government agencies, financial institutions, or health authorities
- Malicious websites themed around covid-19 updates or relief programs (6)
- E-commerce scams involving ppe, sanitizers, or medical supplies
- Fraudulent donation appeals and fake charities
- Cryptocurrency schemes linked to pandemic misinformation (8)

Remote-work arrangements further weakened corporate cybersecurity postures, leading to a surge in business email compromise (BEC) and ransomware attacks (5)(8). The convergence of public health narratives and digital deception marked a new frontier in cyber-enabled fraud.

4.4 Investment and Financial Fraud

Economic volatility and investor uncertainty created conditions conducive to financial fraud. Perpetrators capitalized on pandemic-related themes to promote deceptive investment vehicles (1) (14), including:

- Ponzi schemes disguised as COVID-19 recovery funds (14)
- Speculative ventures claiming involvement in vaccine development
- Cryptocurrency scams promising high returns amid market instability

These schemes often targeted financially distressed or inexperienced investors, leveraging fear and urgency to bypass due diligence (14). The proliferation of such fraud underscores the need for enhanced investor education and regulatory agility during crises.

4.5 Insurance Fraud

The pandemic triggered a surge in health-related insurance claims, some of which were fraudulent. Notable (7) (8) examples included:

- Inflated or fabricated medical billing
- Falsified covid-19 test results and treatment records (11)
- Claims for services not rendered or exaggerated hospitalization costs
- Staged illnesses to trigger policy payouts (7)

Quantitative studies (13)(15) revealed statistical correlations between COVID-19 case spikes and increased insurance fraud attempts. These trends highlight the importance of predictive analytics and claims verification systems in maintaining actuarial integrity during public health emergencies.

4.6 Corporate and Financial Reporting Fraud

Corporate entities facing liquidity constraints and investor pressure engaged in financial misrepresentation to preserve market confidence and access emergency funding (2)(14). Common manipulations included:

- Premature or fictitious revenue recognition
- Inflated asset valuations and understated liabilities
- Misclassification of expenses to enhance profitability
- Distortion of solvency and liquidity indicators

Such practices aimed to secure loans, attract investment, or qualify for government assistance programs. The pandemic thus exposed latent weaknesses in corporate governance and underscored the need for robust audit mechanisms during periods of economic stress (14).

5 COVID-19 and Structural Weaknesses in Global Governance Systems

Emergency relief programs were designed to deliver immediate support to households and businesses. However, the urgency of disbursement often bypassed established due-diligence and accountability mechanisms. While speed was essential to mitigate economic collapse, it inadvertently created opportunities for fraudulent actors to exploit loopholes, siphoning resources away from legitimate beneficiaries (7). The absence of integrated digital identity frameworks and robust verification mechanisms left many governments vulnerable to fraudulent claims. Weak interoperability and poor data-sharing across agencies facilitated duplication, manipulation, and misreporting. This fragmentation underscored the need for secure, unified platforms capable of cross-agency validation.

Fraud, particularly cyber-enabled fraud, transcends national boundaries. During the pandemic, cybercriminals leveraged jurisdictional gaps, exploiting variations in legal frameworks, enforcement capacity, and regulatory reach. The lack of coordinated international oversight highlighted the inadequacy of existing governance structures in addressing transnational threats (8) (12). Lockdowns and remote operations severely constrained the ability of auditors, inspectors, and enforcement agencies to conduct physical checks, site visits, and in-person verifications. Oversight functions were weakened, allowing fraudulent procurement, misallocation of funds, and corruption risks to proliferate under the cover of emergency operations.

Communities with limited digital literacy and access were disproportionately exposed to scams and misinformation. This digital divide amplified the social impact of fraud, compounding vulnerabilities among already disadvantaged groups (5) (6). The inequitable distribution of digital skills and infrastructure became both a governance and social justice issue.

6 Long-Term Implications of Pandemic-Driven Fraud

The surge of fraud during COVID-19 has enduring consequences for public trust, economic stability, and governance systems (7). Beyond immediate financial losses, the pandemic revealed structural vulnerabilities that will shape institutional reforms for years to come.

6.1 Erosion of Public Trust

Fraud in government relief programs undermined confidence in public institutions and fiscal stewardship. Citizens, witnessing misuse of emergency funds, may question the integrity of public spending and the fairness of resource allocation (7). This erosion of trust weakens the legitimacy of future emergency interventions and complicates efforts to mobilize collective compliance during crises.

6.2 Increased Regulatory Burden

In response to pandemic-era fraud, many jurisdictions introduced stricter compliance frameworks, enhanced reporting requirements (10), and more sophisticated identity verification systems. While these reforms strengthen safeguards, they also impose administrative burdens on legitimate businesses and individuals. The challenge lies in balancing fraud prevention with regulatory efficiency to avoid stifling economic recovery and innovation.

6.3 Persistent Cybercrime Infrastructure

Fraud networks established during the pandemic did not dissolve with the crisis. Instead, COVID-19 accelerated the professionalization of cybercrime, embedding sophisticated infrastructures that continue to fuel ransomware, phishing, and identity theft (6). These entrenched networks represent a lasting threat to financial systems, requiring sustained investment in cybersecurity and international cooperation.

6.4 Need for Crisis-Resilient Governance

The pandemic highlighted the tension between rapid economic support and adequate fraud prevention. Future crisis responses must integrate resilience into governance frameworks—combining real-time data analytics, interoperable digital identity systems, and targeted fraud-detection mechanisms (3)(2). Building such adaptive capacity is essential to ensure that emergency interventions remain both swift and secure.

7 Conclusion

The relationship between fraud and the COVID-19 environment is both profound and multifaceted. The pandemic created a rare convergence of conditions—economic hardship (1), rapid digitalization (6), institutional strain(7), and heightened uncertainty(14)—that significantly increased fraud risks worldwide. Through the lens of the Fraud Triangle and Fraud Hexagon, it becomes clear that all elements necessary for fraud—pressure, opportunity, capability, collusion, rationalization, and arrogance—were amplified during this period.

Fraud during COVID-19 manifested across numerous domains, including health care, digital commerce, cybercrime, government relief programs, investment schemes, and corporate reporting (12). The crisis exposed systemic weaknesses in governance, data infrastructure, and regulatory oversight, highlighting the need for more resilient and adaptive systems capable of responding to future emergencies without compromising security (9).

Ultimately, the COVID-19 pandemic serves as a powerful reminder that crises do not merely create suffering, they also create opportunities for exploitation (1). Understanding the relationship between fraud and crisis environments is essential for building stronger, more fraud-resistant institutions in the years ahead.

Compliance with ethical standards

Disclosure of Conflict of interest

No conflict of interest to be disclosed.

References

[1] Zhang Y, Wu Q, Zhang T, Yang L. Vulnerability and fraud: evidence from the COVID-19 pandemic. Humanit Soc Sci Commun. 2022;9(1):424. doi:10.1057/s41599-022-01445-5

[2] Arum EDP, Wijaya R, Wahyudi I, Brilliant AB. Corporate governance and financial statement fraud during the COVID-19: study of companies under special monitoring in Indonesia. J Risk Financ Manag. 2023;16(7):318. doi:10.3390/jrfm16070318

[3] Triyanto DN, Fajri MAN, Wahyuni D. How is financial reporting fraud with the fraud hexagon approach before and during COVID-19 pandemic? J Contemp Account. 2023;5(2):97 114. Available from: https://journal.uii.ac.id/JCA/article/download/28933/15706/98904

[4] Pamungkas ID, Oktafiyani M, Swatyayana PA, Kurniawati R, Putri AA, Alfared MAA. Can corporate governance structures reduce fraudulent financial reporting in the banking sector? Insights from the fraud hexagon framework. J Risk Financ Manag. 2024;18(12):698. doi:10.3390/jrfm18120698

[5] Putra MA, Achmad T. The influence of hexagon fraud theory on fraudulent financial reporting: the moderating role of the audit committee. ResearchGate [Preprint]. 2023. Available from: https://www.researchgate.net/publication/387278640

[6] Noor AAM, Haron NH, Rohani SRS, Rahman R. COVID-19 pandemic and online fraud: Malaysian experience. Int J Acad Res Account Financ Manag Sci. 2022;12(4):192 207. doi:10.6007/IJARAFMS/v12 i4/14172

[7] United States Government Accountability Office (GAO). COVID 19 relief: consequences of fraud and lessons for prevention. GAO 25 107746. Washington (DC): GAO; 2025. Available from: https://www.gao.gov/products/gao-25-107746

[8] Ma KWF, McKinnon T. COVID 19 and cyber fraud: emerging threats during the pandemic. ResearchGate [Preprint]. 2020. Available from: https://www.researchgate.net/publication/344959656

[9] Kumar A, Prasad U, Tiwari RK, Kumar B, Alam M. Impact of the COVID-19 pandemic on healthcare fraud: a comprehensive literature review. In: IGI Global Scientific Publishing; 2023. p. 245 263. Available from: https://www.researchgate.net/publication/386479178

[10] Hill A, Mirchandani M, Pilkington V. Ivermectin for COVID 19: addressing potential bias and medical fraud. Open Forum Infect Dis. 2022;9(2):ofab645. doi:10.1093/ofid/ofab645

[11] Festa MM, Jones MM, Knotts KG. A qualitative review of fraud surrounding COVID 19 relief programs. J Forensic Account Res. 2023;8(1):208 223. doi:10.2308/jfar-2023-11381

[12] Pitchan MA, Salman A, Muhamad Arib N. A systematic literature review on online scams: insights into digital literacy, technological innovations, and victimology. Malays J Commun. 2023;39(1):45 67. Available from: https://ejournal.ukm.my/mjc/article/download/84179/17056

[13] Zhu X, Wang Y, Chang Y, Chen R, Li J. Anti fraud analysis during the COVID 19 pandemic: a global perspective. Int J Inf Technol Decis Mak. 2024;23(1):37 55. doi:10.1142/S0219622023400023

[14] Yazid M, Darsono D. An empirical analysis of asset misappropriation fraud during the COVID 19 pandemic. Probl Perspect Manag. 2024;22(3):145 158. Available from: https://www.businessperspectives.org/images/pdf/applications/publishing/templates/article/assets/20578/PPM_2024_03_Darsono.pdf

[15] Zhu X, Wang Y, Chang Y, Chen R, Li J. Covid 19 and insurance: global comparative perspectives. In: Springer Nature; 2023. Available from: https://link.springer.com/book/10.1007/978-3-031-13753-2