Integrated Journal for Research in Arts and Humanities
ISSN (Online): 2583-1712
Volume- 6 Issue- 2 || March 2026 || PP. 167-169 https://doi.org/10.55544/ijrah.6.2.25

Cyberfraud as Political Economy: Regulation, Enforcement, and Digital Vulnerability in Developing States

Prof. Dr. Stanley Anthony Vivion Paul (Sr.)[1], Prof. Dr. Justin Joseph[2], Prof. Stanley Anthony Vivion Paul (Jr.)[3] and Prof. Orande Kenneatior Solomon[4]

[1]Professor, University of Excellence, Management and Business (U.E.M.B.), Georgetown, GUYANA.
[2]Professor, University of Excellence, Management and Business (U.E.M.B.), Georgetown, GUYANA.
[3]Professor, University of Excellence, Management and Business (U.E.M.B.), Georgetown, GUYANA.
[4]Professor, University of Excellence, Management and Business (U.E.M.B.), Georgetown, GUYANA.

[1]Corresponding Author: principal@uemb.edu.gy

www.ijrah.com || Vol. 6 No. 2 (2026): March Issue

Date of Submission: 15-03-2026	**Date of Acceptance:** 22-03-2026	**Date of Publication:** 25-03-2026

ABSTRACT

This article analyzes cyberfraud not as isolated online deception but as a political-economy problem rooted in weak regulation, transnational criminal infrastructure, and uneven state capacity. It argues that developing states face a distinctive vulnerability because digital adoption has outpaced the institutional maturation of policing, financial intelligence, consumer protection, data governance, and cross-border legal cooperation. Contemporary fraud markets are increasingly industrialized, technology-enabled, and integrated with trafficking, money laundering, and illicit online marketplaces. The article contends that effective response requires a shift from reactive victim-focused policing to system-level disruption of criminal infrastructure. Priority areas include payment surveillance, beneficial ownership transparency, platform accountability, digital literacy, and treaty-based cooperation on electronic evidence. Cyberfraud, in this framing, is not merely a criminal-law issue; it is a governance stress test for digitally exposed but institutionally uneven states.

Keywords- cyberfraud; digital crime; enforcement; organized crime; regulation**.**

I. INTRODUCTION

Cyberfraud has become one of the most pervasive forms of contemporary criminality. It operates through phishing, business email compromise, romance-investment scams, impersonation, account takeover, fake marketplaces, synthetic identities, and increasingly through AI-assisted deception. Yet public discussion still often treats it as a matter of individual carelessness. That explanation is inadequate. Contemporary fraud is structured, scalable, and transnational. INTERPOL's recent threat assessments show that organized crime groups have professionalized fraud operations through low-cost technological tools, cryptocurrency-enabled laundering, and specialized service markets that reduce entry barriers for offenders (INTERPOL, 2024, 2026) (INTERPOL, 2024; Europol, 2024).

Developing states are especially exposed. Digital payments, e-commerce, and remote communication have expanded rapidly, but institutional safeguards have not kept pace. Citizens are drawn into digital systems faster than regulators can supervise them, and law enforcement bodies often confront skilled cross-border actors with limited forensic capacity, fragmented data access, and cumbersome mutual legal assistance procedures (FATF, 2023; United Nations, 2024).

II. FROM FRAUD INCIDENT TO FRAUD INFRASTRUCTURE

The decisive analytical shift is from incident to infrastructure. Cyberfraud does not flourish because many individuals decide independently to send deceptive messages. It flourishes because criminal ecosystems now

Integrated Journal for Research in Arts and Humanities
ISSN (Online): 2583-1712
Volume- 6 Issue- 2 || March 2026 || PP. 167-169 https://doi.org/10.55544/ijrah.6.2.25

combine data brokers, malware vendors, payment mules, illicit call centres, underground banking channels, and laundering mechanisms into integrated supply chains. UNODC has documented how cyber-enabled fraud and underground banking have converged with technological innovation and other organized criminal activities, creating industrial-scale scam architectures with a growing global footprint (UNODC, 2025) (UNODC, 2025; INTERPOL, 2026).

This changes the meaning of enforcement. Arresting low-level operators or issuing public warnings is not enough. Governments must identify and disable the enabling infrastructure: anonymous accounts, shell entities, mule networks, unregulated payment corridors, weak customer due diligence, and non-cooperative digital platforms. The relevant question is therefore not how to punish completed frauds alone, but how to raise systemic friction throughout the fraud economy (Europol, 2024; FATF, 2023).

III. WHY DEVELOPING STATES ARE STRUCTURALLY VULNERABLE

Three structural conditions explain the vulnerability of developing states. First, institutional asymmetry: private technological adaptation moves faster than public regulation. Fraud actors innovate across messaging, deepfakes, spoofing, and social engineering while many regulatory systems still operate with analog assumptions. Second, enforcement fragmentation: telecommunications regulators, financial intelligence units, police, consumer-protection bodies, and prosecutors often work in silos, allowing criminal proceeds and evidence trails to move faster than the state. Third, international dependency: critical data, platforms, and payment architecture frequently sit outside domestic jurisdiction, making electronic evidence and asset recovery difficult (INTERPOL, 2024; Europol, 2024).

The adoption of the United Nations Convention against Cybercrime is significant because it begins to supply a broader framework for cooperation around electronic evidence and cyber-enabled offences, including fraud-related conduct (United Nations, 2024). But treaty architecture alone will not solve the problem. Domestic implementation capacity remains decisive. States need trained investigators, digital evidence protocols, beneficial ownership transparency, and risk-based supervision of banks, fintech operators, and virtual asset service providers (FATF, 2023; United Nations, 2024).

IV. A REGULATORY AND ENFORCEMENT STRATEGY

An effective strategy has five pillars. First, financial disruption. Fraud is sustainable only because proceeds can be moved, layered, and withdrawn. Stronger suspicious transaction monitoring, mule-account detection, rapid freezing powers, and cross-border intelligence exchange are essential. Second, platform responsibility. Messaging, advertising, and marketplace platforms should face escalating obligations around fraud detection, identity integrity, and response times for verified criminal abuse. Third, digital consumer protection. The state must treat digital literacy as preventive infrastructure, especially where first-time users are entering formal financial systems. Fourth, integrated national response. Cybercrime units, telecom regulators, central banks, and prosecutors require standing coordination mechanisms. Fifth, international cooperation. Evidence preservation, extradition, and asset tracing must become faster and more technically competent (UNODC, 2025; INTERPOL, 2026).

The broader policy implication is that cyberfraud should be governed as an ecosystem risk. Where it is treated only as an accumulation of private losses, governments underreact. Where it is seen as a threat to trust in digital finance, e-government, and online commerce, the case for institutional investment becomes much stronger (Europol, 2024; FATF, 2023).

V. FOLLOW-THE-MONEY ENFORCEMENT AND PRIVATE-SECTOR GATEKEEPING

Cyber-enabled fraud is sustainable because it is monetizable at scale. Fraud proceeds are routed through payment processors, mule accounts, crypto-assets, informal value-transfer systems, and shell businesses that convert deception into cash-out capacity. The enforcement implication is straightforward: victim awareness campaigns remain necessary, but they are structurally secondary to financial disruption. Banks, telecom operators, fintech firms, domain registrars, and messaging platforms are part of the fraud-prevention perimeter because they hold the transactional and behavioural signals that states often lack (FATF, 2023; INTERPOL, 2026).

This requires a more mature regulatory settlement between the state and the private sector. High-velocity reporting channels, suspicious-pattern analytics, mule-account typologies, and rapid preservation of digital evidence should become standard obligations rather than exceptional cooperation. Where private actors externalize the cost of fraud onto citizens and law enforcement, cyberfraud markets deepen. Where regulatory design makes prevention a shared compliance duty, criminal profitability falls because speed, anonymity, and volume become harder to sustain (Europol, 2024; FATF, 2023).

Integrated Journal for Research in Arts and Humanities
ISSN (Online): 2583-1712
Volume- 6 Issue- 2 || March 2026 || PP. 167-169 https://doi.org/10.55544/ijrah.6.2.25

VI. CAPACITY, COOPERATION, AND THE GEOGRAPHY OF FRAUD

Developing states face a particular coordination problem: fraud infrastructure is transnational while investigative authority remains territorially fragmented. Scam operations can source victims in one jurisdiction, use infrastructure in another, launder proceeds through a third, and withdraw value in a fourth. International cooperation is therefore not a diplomatic luxury. It is a functional requirement for evidence gathering, extradition, asset tracing, and synchronized disruption. The United Nations Convention against Cybercrime matters in this respect because it aims to create more predictable channels for investigative assistance and evidence-sharing (United Nations, 2024; UNODC, 2025).

Yet legal instruments will underperform if domestic capacity remains thin. Specialist prosecutors, digital forensics, financial intelligence, and victim-reporting systems require continuous investment. States that treat cyberfraud as a narrow IT issue will remain reactive. States that govern it as a blended criminal, financial, and consumer-protection threat are more likely to build institutions capable of disrupting networks rather than merely documenting losses after the fact (INTERPOL, 2024; INTERPOL, 2026).

VII. CONCLUSION

Cyberfraud is no longer a marginal cybercrime. It is a major transnational revenue stream built on digital asymmetry, weak regulation, and scalable deception. Developing states will remain disproportionately vulnerable until they move from reactive policing to infrastructure-focused prevention and disruption. The central task is not only to make fraud illegal, this is already the case, but to make it significantly harder to organize, finance, launder, and repeat (INTERPOL, 2024; Europol, 2024).

REFERENCES

[1] Europol. (2024). Internet organised crime threat assessment (IOCTA) 2024.
[2] Financial Action Task Force. (2023). Illicit financial flows from cyber-enabled fraud.
[3] INTERPOL. (2024). Global financial fraud assessment.
[4] INTERPOL. (2026). Global financial fraud threat assessment.
[5] United Nations. (2024). United Nations convention against cybercrime.
[6] United Nations Office on Drugs and Crime. (2025). Inflection point: Global implications of scam centres, underground banking and illicit online marketplaces in Southeast Asia.