Chapter 7
Policies Against Fraud and Cybercrime:
Strategic, Legal, and Technological Approaches

Radha Ranjan
https://orcid.org/0009-0009-1550-7780
Amity University, Patna, India

Naveen Nandal
https://orcid.org/0009-0007-2272-7437
JIMS, India

Ankit Kumar
https://orcid.org/0009-0001-8249-4969
Sandip University, Sijoul, India

Anupam Sinha
Amity Law School, India

S. Srinivas Kumar
Jain University, India

Shagufta Parween
https://orcid.org/0000-0002-5221-4137
Chaitanya Bharathi Institute of Technology, India

Bhoopathy Rajan
https://orcid.org/0000-0003-2175-6328
Sree Rama Engineering College, India

ABSTRACT

In an age of rapid digitisation, fraud and cybercrime have transformed into intricate risks affecting individuals, enterprises, and governments. The expansion of e-commerce, online banking, and mobile payments

DOI: 10.4018/979-8-3373-5992-2.ch007

has heightened hazards like ransomware, identity theft, phishing, and money laundering, with anticipated losses estimated at USD 10.5 trillion per year by 2025. This paper presents a comprehensive framework that integrates strategic policies, robust regulatory measures, and cutting-edge technologies—AI, machine learning, blockchain, and behavioural analytics—to identify and mitigate fraud. It analyses international rules (e.g., GDPR, CCPA, EU AI Act, FATF AML) and transnational collaboration, supplemented by case studies from the banking, e-commerce, and governmental sectors. Challenges such as adversarial AI, algorithmic bias, and disconnected response systems are tackled, with resilience techniques encompassing adversarial training and privacy-preserving analytics.

1. INTRODUCTION

1.1 Background: The Rising Threat of Fraud and Cybercrime

In recent years, fraud and cybercrime have become significant risks to economic stability, institutional trust, and individual security globally. The global annual cost of cybercrime is anticipated to reach USD 10.5 trillion by 2025, a significant increase from roughly USD 3 trillion in 2015, so establishing it as the world's third-largest economy, following the United States and China (Cybersecurity Ventures, 2025; BD Emerson, 2025). Annual losses exceed USD 1 trillion, mostly impacting industries such as banking, healthcare, and retail (BD Emerson, 2025). The increasing severity of cyberattacks is demonstrated by a 14 percent increase in occurrences in the UK in 2024, with fraud comprising 41 percent of all offences and damages totalling £1.1 billion (Levy, 2025). The World Economic Forum's worldwide Risks Report (2023) identifies cybercrime as a leading worldwide risk for the forthcoming decade, projecting economic damages to exceed USD 9 trillion in 2024 (WEF, 2023). The global average cost of a data breach has increased to between USD 4.5 million and USD 4.9 million, varying by industry, with financial institutions and healthcare at the higher end of the spectrum (BD Emerson, 2025; Indusface, 2025). Simultaneously, Artificial Intelligence (AI) is reshaping the cyber threat