Chapter 5
Financial Cybercrime, FinTech Adoption, and Bank Performance in an Interconnected Indian Economy:
Typologies, Networks, and Systemic Implications

Priyakrushna Mohanty
http://orcid.org/0000-0001-6933-2757
Christ University, Bengaluru, India

Rashi Modi
http://orcid.org/0009-0006-8069-7849
Christ University, Bengaluru, India

Aaleyah Behera
http://orcid.org/0009-0000-3230-2087
Christ University, Bengaluru, India

ABSTRACT

India's rapid expansion of digital finance has transformed payment systems while heightening exposure to financial cybercrime. Real-time payments, platform-based services, and fintech integration have created risk pathways that extend beyond isolated fraud incidents. This study analyses financial cybercrime in India through a systemic lens, mapping evolving fraud typologies, payment-rail vulnerabilities,

DOI: 10.4018/979-8-3373-6244-1.ch005

organised criminal networks, and behavioural asymmetries. It also examines the capacity of regulatory, infrastructural, and enforcement mechanisms to manage these risks under real-time operational constraints. Drawing on a structured synthesis of academic and policy sources, the paper develops the Systemic Cybercrime Mitigation Framework for Digital Finance (SCMF-DF), which integrates prevention, detection, containment, recovery, and adaptive learning to address cybercrime as a financial stability concern.

1. INTRODUCTION

India has transformed the financial environment with respect to the quick introduction of digital payment systems, building one of the largest digital finance environments in the world (Migozzi et al., 2024). Digital payments over the last years have taken over the economic transactions with the digital form having nearly 99.8 percent of total transaction volume in first half of 2025 as per Reserve Bank of India statistics, meaning an overwhelming shift towards cash to cashless forms (Economic Times, 2025). The Unified Payments Interface (UPI) that contributed over 80 percent of digital payments and led to exponential growth in transaction volumes and values has been at the center of this transition and made India a real-time payment leader in the global context (PwC, 2025; NPCI, 2025). Such proliferation has brought about socioeconomic gains such as an increase in financial inclusion, efficiency, and increased access both in urban and rural settings (Mishra et al., 2024). Nevertheless, the network effects facilitating the high-speed value transfer have similarly increased the vulnerabilities, with digital payment systems becoming the large attack surfaces that cybercriminals can exploit to gain money using increasingly sophisticated schemes (Shaji et al., 2024).

Alongside the rapid escalation of financial cybercrime, India's banking sector has undergone a profound transformation driven by FinTech adoption, platform-based service delivery, and real-time payment infrastructures. Innovations such as interoperable payment rails, API-enabled partnerships, and digital-first customer acquisition have reshaped bank performance by expanding transaction volumes, improving cost efficiencies, and accelerating market reach. At the same time, these performance gains are increasingly entangled with heightened exposure to cyber-enabled financial crime, as speed, scale, and system interoperability compress detection and recovery windows. This chapter therefore situates financial cybercrime not only as a security concern, but also as an unintended consequence of performance-oriented digitalisation in banking, where FinTech adoption simultaneously enhances operational efficiency and amplifies systemic financial risk.