# Chapter 85
# Are the Payments System and e-Banking in India Safer than in other SAARC Members?

**Rituparna Das**
*University of Petroleum and Energy Studies, India*

## ABSTRACT

*This paper deals with the issues in the way the banks are managing risks in payments and settlement systems using netbanking within the legal frame of information technology in India compared to other SAARC members. It compared India with the SAARC members with respect to management of credit risk, liquidity risk and operational risk in the payment system. The findings are: (i) India, Pakistan and Nepal are stronger in managing all of aforesaid risks in their payments systems relative to the rest and (ii) India is the most permissive by nature as to the crime of computer hacking.*

## INTRODUCTION

Electronic banking (e-banking) is synonymous with internet banking (i-banking) from the user viewpoint when it comes to online (i) distribution of banking products by banks and (ii) payments and receipts of funds by banks as well as users. In India electronic banking expanded as a result of the internet communication technology revolution. Because a major driving force behind the rapid spread of i-banking all over the world is its acceptance as an extremely cost effective delivery channel of banking services as compared to other existing channels, after studying the experiences faced by USA, UK and Scandinavian Countries and taking assistance from the leading Indian multinational IT (information technology) company Infosys Limited the Reserve Bank of India (RBI) designed regulatory and technological frameworks for India, which the banks need to follow. The statistics on payments, clearing and settlement systems in the countries who follow the guidelines of CPSS (Committee on Payment and Settlement Systems) are available in Bank for International Settlements (2011).

DOI: 10.4018/978-1-7998-1760-4.ch085

The rest of the paper critically discusses the anatomy of the electronic payment system in India compared India to other SAARC members in matter of managing credit risk, liquidity risk and operational risk from regulatory view point and examines the ease of hacking one's e-banking account from a hacker's perspective through axiomatic approach.

## BACKGROUND

The onset of electronic banking (e-banking) in India dates back to 2001 after five years of commencement of electronic clearing service in 1995. Different innovations in this field include RTGS (Real Time Gross Settlement System), NEFTS (National Electronic Fund Transfer System), CTS (Cheque Truncation System), NECS (National Electronic Clearing Service), mobile banking and satellite banking. In the current decade by and large all commercial banks in India are offering internet banking, mobile banking and ATM facilities. In any Indian commercial bank (henceforth 'bank') governance of IT is a *part and parcel* of its corporate governance. Every such bank has an independent IT Committee with professionally qualified members. This Committee participates in the Board of Directors and manages all the risks related to IT at the enterprise level.

The needs for mitigation of credit risk in securities settlements and reduction in interest cost of slow speed in physical payments gave birth to the electronic payment and settlement systems. The second benefit of these systems is that they facilitate better management of operational and liquidity risks. The third benefit is that they help faster operations in cross border financial markets. But in the context of exposure to these markets one important lesson learnt from the history of financial crises is that the payment and settlement systems work as a channel through which business risk transmits and in the process, on many occasions, there is conversion of one category of risk to another, e.g. operational risk may change into market risk. A corollary of the above lesson is that through payment and settlement systems a single category of risk at the point of origin is distributed as multiple categories among the receivers. Other related lessons are that (i) categorization of business risk depends on the types of system design and settlement method, and (ii) it varies from case to case whether the settlement system alone has to bear the risk, share it with clients or bounce back to clients.

In India the banking regulator the RBI is at present in the process of addressing the following risks of payment systems - concentration risk, counter-party risk, credit risk, legal risk, liquidity risk, operational risk, regulatory risk, settlement risk and systemic risk. But during the last one year the Deputy Governors of the RBI expressed more concern about operational risk than other risks in their lectures on online banking and electronic payments. Because of the factors typical to emerging economies, like financial exclusion of a sizeable chunk of households, existence of informal sector, a massive parallel economy and availability of education on IT to a tiny privileged section of the population, other risks could not yet attract attention in the Indian context while online frauds like hacking, leaking database and phishing mostly having been engineered offshore, but involving onshore agents, have been receiving attention.

Therefore, being empowered by the Payment and Settlement Systems Act, 2007, the RBI requires every bank to (i) pursue eight basic principles of information security – confidentiality, integrity, authenticity, non-repudiation, identification, authorization, accountability and auditability, and (ii) identify its security requirements in line with the prescription of the CPSS constituted by the Bank for International Settlements (BIS). In the process a bank needs to detect the threats to information database, explore its vulnerability to security threats and the likelihood of occurrence of such threats, assess the potential