ADMISSIBILITY OF DIGITAL FINANCIAL LEDGERS: NAVIGATING ELECTRONIC EVIDENCE STANDARDS UNDER SECTION 61 OF THE BHARATIYA SAKSHYA ADHINIYAM, 2023

Rishav Tater, JIS University, West Bengal[1]

ABSTRACT

The transition of corporate financial documentation from physical ledger books to cloud-based Enterprise Resource Planning (ERP) systems has fundamentally altered the landscape of corporate litigation. With the enactment of the Bharatiya Sakshya Adhiniyam (BSA), 2023, which replaced the Indian Evidence Act, 1872 with effect from July 1, 2024, the Indian legislature has redefined the evidentiary threshold for digital records. This article critically analyses the admissibility of digital financial ledgers under Section 61 of the BSA, read conjunctively with the stringent certification mandate of Section 63. By examining the legislative introduction of hash values and the dual-signature requirement — involving both the person in charge of the device and a technical expert — this paper explores the practical friction these rules create for decentralized, multi-user accounting software such as Tally and for cloud-hosted databases more broadly. It further evaluates the intersection of the BSA's electronic evidence standards with the Ministry of Corporate Affairs' mandate for a non-tamper able audit trail under the Companies (Accounts) Rules, 2014. Ultimately, the article argues that while the BSA seeks to safeguard the forensic integrity of electronic records in white-collar and insolvency litigation, it places an unprecedented procedural burden on corporate governance and statutory compliance structures — one that litigants and resolution professionals alike must anticipate long before a dispute reaches the courtroom.

I. Introduction

In contemporary corporate litigation, disputes are rarely fought over physical ledgers or handwritten entry books. Whether in cases of corporate fraud, insolvency proceedings under the Insolvency and Bankruptcy Code, 2016 (“IBC”), or commercial contract breaches, the core evidentiary battles now revolve around digital footprints. Financial truth is extracted from server logs, cloud-based spreadsheets, and complex Enterprise Resource Planning (ERP) accounting software rather than from bound registers.

For over two decades, the admissibility of such electronic records was governed by the often-litigated Section 65B of the Indian Evidence Act (IEA), 1872. The jurisprudence surrounding Section 65B was notoriously volatile, culminating in the Supreme Court's landmark ruling in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, which cemented the mandatory nature of the electronic certificate.[2] However, recognizing the limitations of a colonial-era statute in adapting to cloud computing and dynamic data, Parliament enacted the Bharatiya Sakshya Adhiniyam (BSA), 2023.

The BSA, effective from July 1, 2024, represents a paradigm shift.[3] Section 61 of the BSA unequivocally guarantees the admissibility of electronic or digital records, ensuring that they cannot be denied admission solely on the ground of their digital nature.[4] That guarantee is, however, strictly tethered to the procedural compliance detailed in Section 63. The new statutory framework introduces rigorous mechanisms — specifically, the mandatory inclusion of a digital hash value and a dual-signature certification process — to authenticate digital documents. This article analyses how these standards under Sections 61 and 63 impact the admissibility of digital financial ledgers, and highlights the friction between strict legal compliance and the fluid reality of modern corporate accounting.

---

[1] LL.B., JIS University, West Bengal.

[2] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 (India).

[3] Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, Acts of Parliament, 2023 (India).

[4] Bharatiya Sakshya Adhiniyam, 2023, Section 61, No. 47 of 2023, Acts of Parliament, 2023 (India).

II. The Anatomy of Section 61 and the Section 63 Certification Mandate

The legislative intent behind Section 61 of the BSA is to place digital documents on the same legal footing as primary paper evidence, thereby mitigating judicial reluctance to rely on intangible data. Section 61 states in clear terms that an electronic or digital record shall have the same legal effect, validity, and enforceability as any other document, subject to the conditions prescribed in Section 63.[5]

Admissibility, however, is not synonymous with proof. The true gateway to admission is Section 63(4), which is the successor to the old Section 65B(4) of the IEA.[6] Section 63(2) retains the foundational requirements carried over from the earlier regime: the computer output must be produced during a period over which the device was in regular use; information must have been fed into it in the ordinary course of business; and the device must have been operating properly, so as to ensure the accuracy of the resulting record.[7]

Where the BSA departs sharply from its predecessor is in the procedural execution of the certificate. Under the former regime, a certificate signed by a person occupying a responsible official position in relation to the operation of the device was sufficient. The BSA imposes a markedly stricter standard: the Schedule appended to Section 63 requires that the certificate be signed by two persons — the individual in charge of the computer or communication device, and a technical expert.

The BSA further introduces the requirement of a "hash value." A hash value functions as the digital fingerprint of an electronic file; any alteration to the underlying data, however minute, changes the resulting hash value.[8] By embedding this requirement into the Section 63 certificate, the legislature has effectively demanded cryptographic proof of a ledger's integrity as a precondition to its admissibility. While this innovation drastically reduces the risk of tampered financial records entering the courtroom, it fundamentally disrupts the manner in which corporations have historically tendered financial printouts in commercial litigation.

---

[5] *Id.*

[6] Compare Bharatiya Sakshya Adhiniyam, 2023, Section 63(4), No. 47 of 2023, Acts of Parliament, 2023 (India), with Indian Evidence Act, 1872, Section 65B (4), No. 1, Acts of Parliament, 1872 (India) (repealed 2024).

[7] Bharatiya Sakshya Adhiniyam, 2023, Section 63(2), No. 47 of 2023, Acts of Parliament, 2023 (India).

[8] Bharatiya Sakshya Adhiniyam, 2023, Schedule, No. 47 of 2023, Acts of Parliament, 2023 (India) (prescribing the format and signatory requirements for the electronic evidence certificate).

III. The Cloud Conundrum: ERP Systems and Corporate Auditing

The rigid technical parameters of Section 63 create considerable operational friction when applied to modern corporate auditing and accounting infrastructure. In mid-to-large corporations, financial records are rarely generated on a single, standalone computer. Books of account are instead maintained on decentralized accounting architectures, were multiple authorized personnel — ranging from data-entry clerks and statutory auditors to the Chief Financial Officer — simultaneously input, modify, and verify data across a cloud network.

This multi-user environment complicates the “lawful control” and “regular course of activities” conditions mandated by Section 63(2)(a) and (b).[9] When GST returns, income-tax documentation, and Registrar of Companies (ROC) compliance forms are all synthesized from a single cloud-hosted ledger, identifying the singular “person in charge” of the device becomes legally ambiguous. Is that person the IT administrator who maintains the server, the statutory auditor who finalizes the balance sheet, or the managing director who bears overarching legal responsibility for the company's books? The statute offers no clear answer, leaving courts to resolve the question on a case-by-case basis.

The dual-signature requirement compounds this difficulty in routine financial litigation. Requiring an independent “expert” to co-sign the certificate for ordinary financial ledgers extracted from accounting software imposes a real evidentiary and financial burden on litigants, particularly small and mid-sized enterprises that may not retain in-house forensic capability.

This friction is compounded further by the Ministry of Corporate Affairs (MCA) mandate under the Companies (Accounts) Rules, 2014, which requires companies to use accounting software equipped with a non-tamper able “Audit Trail” (edit log).[10] The audit trail records every modification made to a financial entry, logging the date, time, and identity of the user responsible. Read together with the MCA's audit-trail mandate, Section 63 of the BSA effectively invites courts to treat the software's internal audit log as the baseline against which the integrity of the certified hash value is assessed. If the hash value stated in the Section 63 certificate does not align with the

[9]Bharatiya Sakshya Adhiniyam, 2023, Section 63(2)(a)–(b), No. 47 of 2023, Acts of Parliament, 2023 (India).
[10]Companies (Accounts) Rules, 2014, R. 3(1) (India) (mandating the use of accounting software with an audit trail feature for companies).

unaltered state of the MCA-mandated edit log, the financial ledger risks being ruled inadmissible — a result capable of collapsing a litigant's entire corporate case on a purely procedural footing.

IV. Strategic Implications for Corporate Litigation

The intersection of financial auditing and the BSA's electronic evidence standards is likely to shape the outcome of modern corporate litigation in at least two specific domains: insolvency proceedings and white-collar defense.

A. Insolvency and Bankruptcy Code Proceedings. In proceedings before the National Company Law Tribunal (NCLT), Resolution Professionals (RPs) frequently rely on a corporate debtor's digital ledgers to identify and reverse preferential, undervalued, or fraudulent transactions under Sections 43 to 66 of the IBC.[11] An RP often inherits a fragmented IT infrastructure from a hostile or uncooperative suspended board of directors. Where the RP seeks to present extracted financial data to prove the fraudulent siphoning of funds, that data must still satisfy Section 63 of the BSA. Generating a valid certificate with a verifiable hash value for historical data created before the RP assumed control is, in practice, technologically demanding. A failure to strictly comply with the BSA's dual-signature and hash-value requirements hands the defense a procedural route by which to strike down the ledgers, thereby shielding potentially fraudulent transactions from substantive judicial scrutiny.

B. White-Collar Crime and Statutory Compliance. In prosecutions involving corporate fraud or systemic tax evasion, investigating agencies rely heavily on digital devices seized during raids. Where prosecuting agencies rely on mirrored hard drives or extracted Tally databases, the defense will closely scrutinize the accompanying Section 63 certificate. If the investigating agency fails to maintain an unbroken chain of custody — resulting in a mismatch between the hash value recorded at the time of seizure and the hash value recorded at the time of production in court — the electronic ledger becomes vulnerable to exclusion. Corporate defense strategy is therefore likely to shift, in appropriate cases, from contesting the substantive merits of an alleged financial discrepancy to attacking the procedural compliance of the Section 63 certificate itself.

[11] Insolvency and Bankruptcy Code, 2016, Section 43–66, No. 31 of 2016, Acts of Parliament, 2016 (India).

V. Conclusion

The Bharatiya Sakshya Adhiniyam, 2023 represents a necessary evolution in Indian evidentiary law, aligning courtroom practice with the realities of the digital economy. By guaranteeing the admissibility of electronic records under Section 61 while demanding cryptographic authenticity through Section 63, the legislature has built a meaningful safeguard against digital tampering.[12]

That heightened evidentiary threshold, however, places a substantial burden on corporate governance. Litigation readiness can no longer begin only once a dispute is filed; it must instead be embedded directly into a company's day-to-day statutory audit and compliance framework. Corporations should proactively restructure their IT and accounting protocols so that whoever manages their digital books is structurally and technically prepared to generate a compliant, dual-signed Section 63 certificate at short notice. In the present era of commercial litigation, the strength of a financial claim is increasingly only as strong as the digital fingerprint of the ledger that supports it.

[12]See generally Tomaso Bruno v. State of Uttar Pradesh, (2015) 7 SCC 178 (India) (discussing the necessity and reliability of electronic evidence in modern adjudication)