NEWSLETTER

15TH EDITION, AUGUST 2026

SALOT & SHAH
ASSOCIATES

Welcome to the 15th edition of our Newsletter. Through this edition, we aim to keep our clients and readers updated of significant legal developments, evolving trends, and key insights shaping the legal landscape, along with practical perspectives on their implications.

As businesses operate in an increasingly digital and interconnected world, legal risk has evolved from a compliance issue into a strategic business priority. This edition explores three critical developments shaping modern commerce: third-party vendor liability and cyber risks, the legal challenges of AI-generated commercial content and synthetic identity misuse, and the growing preference for institutional arbitration in commercial disputes. Together, these articles offer practical insights to help business leaders strengthen governance, reduce legal exposure, and build resilient, future-ready enterprises.

Contact
Ph.+91 93286 69090
info@salotandshah.com
www.salotandshah.com
Office: 503, 5th Floor, Phoenix Towers, Opp. New Girish Cold Drinks, Vijay X Roads, to Commerce Six Road, Navrangpura, Ahmedabad, Gujarat- 380009.

VENDOR BREACHES AND THIRD-PARTY CYBER RISKS: WHO BEARS THE LIABILITY?

INTRODUCTION:

Modern businesses increasingly depend on third-party vendors for cloud storage, payroll management, software operations, customer databases, payment gateways, and communication systems. While the outsourcing process improves the efficiency and scalability, it also creates the risk of cyberattacks. A breach at a vendor's system can indirectly expose a company's customer information, disrupt business operations, damage reputation and trigger legal as well as financial liability breach at a vendor's system can indirectly expose a company's customer information, disrupt business operations, damage reputation, and trigger legal as well as financial liability. The growing dependence on external service providers has therefore transformed vendor cybersecurity into a core governance issue.

THE GROWING RISK OF VENDOR-DRIVEN CYBER BREACHES

Third-party cyber breaches actually happen when there is a condition where an external supplier, contractor, software provider, or any cloud service partner suffers a cyber incident that ultimately affects the business using those services. Also, these incidents create a cascading effect across the industries because businesses operate digitally in a connected ecosystem in today's time.

The third-party vendors these days, occupy a critical position within the corporate operations. They primarily manage the payroll systems, customer databases, reservations for platforms, email infrastructure, payment processing and cloud hosting services. Ultimately if there is a time where a vendor experiences a weak security control or any kind of system vulnerabilities, the associated business may also become exposed to such threats. The famous Marriott breach remains one of the most crucial and significant examples of vendor- related cyber vulnerability case.

In this, the Hackers exploited the vulnerabilities in the Starwood's reservation system, exposing nearly 500 million guest records and the regulators argued that a deeper vendor due diligence and security assessments should have been conducted before integration

LEGAL RESPONSIBILITY BEYOND THE BREACH

One of the most significant issues that surrounds the third-party breaches concerns liability allocation. The businesses often assume that the responsibility lies in the sole onus of the vendor that suffers the breach. However, the lability primarily extends to the principal company if it failed to conduct an adequate vendor due diligence or neglected to implement proper cybersecurity oversight mechanism. It is pertinent to note that negligence remains the central principle that governs cyber liability and if an organization somewhere fails to evaluate a vendor's security posture, ignores cybersecurity weaknesses or enters contracts that lack clear allocation provisions, regulators and courts may still hold the business accountable in these cases.

The contractual agreements become very critical in determining the liability exposure A fortified indemnity clause, a breach notification obligation, audit rights and any shared responsibility provisions may significantly reduce risk exposure. There are several businesses that have successfully recovered losses from the vendors because their contracts included hold harmless protections and cyber security compliance obligations. to sum up, A poorly drafted agreement in majority times leave the organizations very prone to litigation costs and operational losses in long run.

The cyber insurance has emerged as one of the major mechanisms for a vendor related cyber exposure. The traditional business interruption Insurance generally covers losses that result from cyber incidents directly affecting a company's own systems. However, it is pertinent to note that this coverage may not extend to losses caused by disruptions at external suppliers or any service providers. In order to address this gap, the businesses are increasingly relying upon contingent business interruption insurance protecting the organizations from financial losses arising from cyber incidents suffered by the third-party vendors.

THE EVOLVING LANDSCAPE OF VENDOR CYBER RISK

CBI Policy often contains narrower terms, longer waiting periods, lower payout limits and Exclusions that are related to partial operational slowdowns. The businesses should always be very careful while reviewing the policy and must understand the scope of coverage available for vendor related incidents. The growing importance of vendor Dependency has made cyber insurance evaluation component of risk management.

The cyber breach rarely creates only technical damage but they also generate a severe reputational consequence against the organization. The public trust often declines very sharply after customer data exposure, especially when business appears unprepared or failed to communicate transparently or in a convincing manner to the customers. Organizations that are affected by the vendor related breaches should always implement effective crisis communication strategies involving timely disclosure a very clear-cut remediation measures and public communication.

An increased adoption of artificial intelligence has come up with additional complexities within vendor related cyber risks. AI systems frequently operate through the third-party software providers, an automated decision-making platform and cloud-based data processing systems failures within AI driven vendor ecosystems may also expose businesses to some new categories of liability that involves algorithmic bias or inaccurate automated decisions and privacy risks.

FROM DUE DILIGENCE TO CONTINUOUS MONITORING

The businesses cannot completely eradicate or eliminate vendor related cyber risks, but they can significantly reduce the exposure through proactive governance measures. A vendor assessment should be conducted before engagement and should be monitored continuously and thoroughly thereafter. Cyber security certifications, penetration testing reports, access control systems and also compliance records must be reviewed on a regular basis.

Businesses can significantly reduce vendor-related cyber risks by implementing multi-factor authentication and strong access controls, conducting regular cybersecurity audits and penetration testing, training employees regarding phishing attacks and vendor-related threats, developing incident response plans involving third-party breach scenarios, and undertaking annual reviews of cyber insurance policies to address evolving vendor dependencies

CONCLUSION

The third-party vendor breaches have now become one of the most serious cyber security threats facing the modern businesses. Vendor negligence, a weak contractual-protection clause may be an inadequate cyber security oversight and evolving AI related risks collectively expand organizational exposure to these cyber risks. While cyber insurance and contractual safeguards provide important protection mechanisms they cannot really eradicate or eliminate entirely the liability or reputational harm which is inevitable. To control this or in order limit the harm businesses must therefore adopt a proactive approach that combines vendor due diligence with contractual risk allocation, cyber security governance, crisis preparedness and a regular monitoring procedure.[1]

THE GROWING EMPHASIS UPON INSTITUTIONAL ARBITRATION FOR COMMERCIAL ENFORCEMENTS

INTRODUCTION:

Businesses in today's fast-moving economies and commercial environment can't afford a prolonged delay in commercial recoveries. Essential parts of commercial stability are required in every sector, whether it's a financial institution recovery or a manufacturing unit dealing with vendors, this goes beyond the cross-border commercial relationships, which requires a efficient disputes resolution mechanisms. The High Court of Rajasthan in one of its recent ruling dealings with such commercial recovery transactions through an Institutional Arbitration attracted a significant attention and laid rulings regarding the importance of institutional arbitration. In an increasingly contract – driven economy this ruling clarifies the legal positioning surrounded around the institutional appointment of arbitrators along with this it is also developed a confidence in arbitration as a practical mechanism which is very much enforceable also in the eyes of law.

DISPUTE RESOLUTION IS AN IMPORTANT ASPECT FOR GROWING BUSSINESSES

The pace and scale of commercial relationships have grown significantly in today's economy. Businesses regularly enter into vendor contracts, software service agreements, franchise arrangements, and financing transactions across industries and borders. Whether it is an IT company serving overseas clients, a manufacturer relying on supply chains, a hospital managing vendors, or an AI platform onboarding third-party service providers, every business depends on one critical factor: the enforceability of agreements. A contract has real value only when there is an effective mechanism to resolve disputes and recover dues.

WHY HAS ARBITRATION BECOME IMPORTANT FOR BANKS AND NBFCS?

Banks and Non-Banking Financial Companies (NBFCs) have relied heavily on arbitration for recovery of small and medium-sized loan defaults. Since these institutions deal with public money and credit circulation, speedy recovery of dues becomes commercially necessary. Arbitration offered a quicker mechanism for recovery and enforcement.

The practice of appointment of a sole arbitrator by one party in a commercial relationship is a traditional practice for many businesses, lenders and institutions by simply including a clause in their contracts, this practice has been common across industries for years now. However, it has raised concerns over its neutrality, which is lacking, and also concerns about the fairness of such appointments, which are arbitrary for the other party's interests and do not provide a proper mechanism for dispute resolution.

The major development was when the highest court of the country delivered an important ruling in *TRF Ltd. V. Energo Engineering Projects Ltd [(2017) 8 SCC 377]*, and *Perkins Eastman Architects DPC v. HSCC (India) Ltd [AIR (2020) SC 59]*, here the contentions of the supreme court clearly stated that "a party in the contract cant appoint a sole arbitrator unilaterally as a outcome of a clause for arbitration " the reasoning was simple that arbitration must remain a independent and neutral aspect , free from any perception of biasness and arbitrary actions.

After these judgements, banks, NBFCs and several commercial organizations started moving towards institutional arbitration models. Instead of directly appointing arbitrators themselves, disputes began getting referred to arbitration institutions that independently appoint arbitrators under their own procedural systems.

THE PROBLEM FACED DURING THE ENFORCEMENT OF AWARDS:

Several execution courts across India started questioning arbitral awards even where arbitrators were appointed through institutions. In many cases, courts treated institutional appointments as indirect forms of unilateral appointments and refused enforcement of arbitral awards. This created serious commercial uncertainty. The issue became even more significant for smaller NBFCs because they do not receive the benefit of the SARFAESI Act for loan amounts below Rs. 20 Lakhs. As a result, arbitration often remained their primary legal remedy for recovery.

THE PROBLEM FACED DURING THE ENFORCEMENT OF AWARDS:

In this background, the recent judgement of the Rajasthan High Court while dealing with a civil miscellaneous writ petition in Sundaram Finance Ltd vs Hanuman Prasad and Anr , was delivered on 24th April this year has become highly significant. The dispute arose from a vehicle loan transaction where the borrower defaulted in repayment. As per the arbitration clause in the agreement, disputes were to be referred to the Madras Chamber of Commerce and Industry (MCCI) in 2022, which would appoint the arbitrator.

The institution accordingly appointed a sole arbitrator, and an arbitral award was passed in favour of the lender. However, during enforcement proceedings, the execution court dismissed the award on the ground that the appointment was allegedly unilateral. The lower court also questioned the jurisdiction of Chennai as the seat of arbitration in the contract; the execution court could not invalidate the proceedings merely because the borrowers resided elsewhere.

WHY THIS JUDGEMENT MATTERS BEYOND THE BANKING SECTOR?

This judgement is not only important for the banks and NBFCs but for the businesses across industries. The ruling reinforces the growing importance of properly structured dispute resolution clauses. Today, businesses are rarely limited to geographical boundaries. IT companies work with international clients, manufacturers depend on cross-border procurement, hospitality businesses rely on multiple vendor ecosystems, educational institutions collaborate globally, and AI-driven platforms regularly engage third-party developers and consultants.

From a legal advisory firm's perspective, this judgement highlights why businesses should now carefully revisit their agreements, especially arbitration clauses contained in vendor contracts, software licensing agreements, consultancy agreements, franchise arrangements, infrastructure contracts, and international commercial arrangements.

A poorly drafted arbitration clause may appear insignificant during negotiations, but during an actual dispute, it can delay recovery, increase litigation costs, and weaken enforceability entirely.

THE NEED FOR CAREFUL DRAFTING & GENUINE INSTITUTIONAL MECHANISM:

Courts are still likely to examine whether the institutions functions independently or merely acts as a mechanism indirectly controlled by one party. The Madras High Court judgement in *Thomas Varghese v. Sundaraman Finance Ltd* was delivered on 24th February earlier this year, it also cautioned courts to distinguish between genuine arbitral institutions and arrangements created merely to bypass restrictions on unilateral appointments. That is why a careful drafting of legal clauses has become important in today's time. As per the evolving judicial standards, it's a duty for Businesses that they must ensure that arbitration clauses in their contracts are enforceable and balanced, showcasing an adaptability for a practical approach that aligns with their commercial needs.

The framework of Arbitration is developing as a greater aspect of neutrality with commercial practicality implications and an institutional approach. A need for fast, enforceable and commercially realistic dispute resolution mechanisms is the need of every business in India today, which is also very well represented and showcased through the judgement of the High Court of Rajasthan as it dives deep into an approach that is evolving and reflects a confidence that is strengthening the objective of institutional arbitration, which sets out to resort a credible modern commercial dispute resolution mechanism. It is a business necessity as per the increase in complex commercial relationships. As it is no luxury for certainty in enforcement for those in the businesses who are navigating their way forward in such complex relationships.

THE ALGORITHMIC DEFAMATION AND CORPORATE LIABILITY: THE EMERGING LEGAL CRISIS OF AI-GENERATED COMMERCIAL MISREPRESENTATION

INTRODUCTION:

Artificial Intelligence has moved beyond automation and analytics into the realm of autonomous commercial representation. Businesses now increasingly use AI-generated advertisements, virtual spokespersons, automated customer interactions, deepfake promotional content, AI-driven branding, and algorithmic decision-making to drive growth. While these technologies improve efficiency and scalability, they also create significant legal risks, including algorithmic defamation, synthetic identity fraud, misleading commercial representation, and unauthorised use of an individual's identity or likeness.

One of the most alarming legal developments emerging globally is the increasing misuse of generative AI systems for creating fabricated commercial communications capable of causing reputational destruction, market manipulation, consumer deception, and institutional fraud on an unprecedented scale. AI-generated false statements, manipulated executive videos, fabricated endorsements, cloned brand identities, synthetic customer reviews, and forged corporate communications are now capable of circulating instantaneously across digital ecosystems with significant commercial consequences.

The legal system is therefore confronted with a fundamental question: where an artificial intelligence system autonomously generates false, misleading, defamatory, deceptive, or commercially manipulative content, who bears legal liability? The developer, the deploying corporation, the platform intermediary, the user operating the system, or all entities collectively involved in the dissemination chain? This issue has now evolved into a major corporate governance, intellectual property, cyber law, and regulatory compliance concern.

ALGORITHMIC DEFAMATION AND AI-GENERATED COMMERCIAL HARM:

Traditional defamation jurisprudence was historically designed around identifiable human actors making false statements with malicious intent or negligent disregard for truth. However, generative AI systems have disrupted this legal foundation by enabling

automated creation of misleading narratives, fabricated allegations, manipulated interviews, and synthetic visual evidence without direct human drafting. Corporations today face increasing instances where AI-generated content falsely attributes statements to directors, promoters, celebrities, institutions, or competing businesses. AI-generated deepfake content, including fabricated executive statements, manipulated merger-related interviews, falsified insolvency disclosures, and synthetic audiovisual recordings designed to distort market perception, is increasingly being utilized as a sophisticated tool for commercial manipulation and investor influence.

The issue becomes particularly severe where AI-generated defamatory content impacts:

1. stock valuation and investor confidence;
2. brand goodwill and commercial reputation;
3. customer trust and market perception;
4. contractual negotiations and business relationships; and
5. regulatory scrutiny and institutional credibility.

Under existing legal principles, corporations may potentially face exposure under defamation law, unfair trade practice regulations, intermediary liability frameworks, cybercrime statutes, securities regulations, and tortious liability principles. The difficulty, however, lies in attribution of liability. AI systems function through probabilistic generation models trained upon massive datasets. Consequently, establishing intentional malice, authorship, and direct causation becomes significantly complicated in algorithmically generated publications.

SYNTHETIC IDENTITY FRAUD AND UNAUTHORIZED PERSONALITY COMMERCIALIZATION:

A particularly dangerous development in 2026 concerns synthetic identity fraud involving unauthorized digital replication of real individuals for commercial exploitation. Generative AI systems are now capable of reproducing:

1. facial identity and expressions;
2. voice patterns and speech modulation;
3. gestures and behavioral characteristics;
4. signature styles and professional communication patterns; and
5. realistic audiovisual appearances.

As a result, businesses increasingly face legal disputes concerning unauthorized AI-generated endorsements, fabricated celebrity promotions, cloned executive representations, and false commercial affiliations. Such conduct raises serious concerns relating to:

1. personality rights infringement;
2. passing off;
3. trademark dilution;
4. false endorsement liability;
5. deceptive advertising practices;
6. privacy violations; and
7. cyber fraud offences.

The absence of comprehensive AI-specific legislation in several jurisdictions has further intensified enforcement challenges. Existing intellectual property frameworks were not originally structured to address synthetic human replication generated through machine learning systems. Consequently, corporations deploying AI-generated marketing content without rigorous legal vetting may inadvertently expose themselves to massive reputational, regulatory, and financial liability.

CORPORATE GOVERNANCE FAILURES AND BOARD-LEVEL EXPOSURE:

Artificial Intelligence is no longer merely a technological function delegated to operational teams. It has now become a governance-sensitive enterprise risk capable of impacting shareholder value, regulatory compliance, institutional integrity, and public accountability. Boards of Directors are increasingly expected to establish governance frameworks addressing:

1. AI deployment oversight;
2. misinformation risk management;
3. synthetic media verification systems;
4. cybersecurity compliance;
5. algorithmic accountability;
6. data governance and privacy protection;
7. intellectual property enforcement; and
8. internal AI usage regulation.

Failure to implement adequate safeguards may expose companies and senior management to allegations of negligence, breach of fiduciary obligations, compliance failures, and reckless governance practices. The legal expectation surrounding corporate governance in 2026 is gradually shifting from passive technological adoption toward active institutional supervision of algorithmic systems. Corporations can no longer rely upon the defense that harmful content was "automatically generated" by an AI tool. Where organizations commercially benefit from automated systems, regulators and courts may increasingly impose corresponding duties of supervision, verification, and risk mitigation.

EMERGING ENFORCEMENT AND REGULATORY TRENDS:

Global regulatory authorities are rapidly moving toward stricter AI accountability standards emphasizing transparency, traceability, explainability, and institutional responsibility. Regulators are increasingly focusing upon:

1. mandatory disclosure of AI-generated content;
2. watermarking and synthetic media identification;
3. intermediary due diligence obligations;
4. platform accountability mechanisms;
5. AI risk classification systems;
6. automated decision transparency; and
7. governance obligations for high-risk AI deployment.

Simultaneously, courts are increasingly recognizing that AI-related commercial harm cannot remain beyond the scope of traditional legal accountability merely because of technological complexity. In India, although dedicated AI legislation remains under development, existing statutory frameworks including the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, the Trade Marks Act, 1999, the Copyright Act, 1957, consumer protection laws, cybercrime provisions, and tortious liability principles may collectively operate to regulate AI-generated misconduct. Therefore, businesses deploying AI systems without comprehensive compliance mechanisms may face substantial litigation exposure in the near future.

CONCLUSION

The intersection of Artificial Intelligence, algorithmic misinformation, synthetic identity fraud, and corporate accountability represents one of the most significant legal crises emerging in 2026. The danger no longer lies merely in AI replacing operational functions; the greater concern lies in AI autonomously influencing public perception, commercial reputation, financial behavior, and institutional trust through fabricated yet highly convincing synthetic content. Modern corporations must therefore transition from reactive legal enforcement toward proactive AI governance and digital risk management. Businesses that fail to establish strong internal AI compliance structures, content verification systems, intellectual property protection mechanisms, cybersecurity protocols, and board-level oversight frameworks may soon encounter severe regulatory intervention, reputational collapse, and high-value commercial litigation. In the evolving legal ecosystem, Artificial Intelligence is no longer merely a technological innovation — it has become a direct subject of corporate liability, governance accountability, and institutional legal scrutiny.

*****