



MEASURING THE GAP: A FOUR-BENCHMARK COMPARATIVE ASSESSMENT OF AI-DRIVEN BANKING FRAUD LAW IN INDIA, THE USA, AND THE UK

Pushkar Sejwal¹ and Dr Meenu Gupta²

¹PhD Scholar, Amity Law School, Amity University, Noida, Uttar Pradesh, India

²Professor, Amity Law School, Amity University, Noida, Uttar Pradesh, India

<https://doi.org/10.5281/zenodo.23366073>

ABSTRACT

Generative artificial intelligence has altered the way banks are defrauded, though not, in most jurisdictions, the legal text that governs it. This paper offers a comparative doctrinal analysis of the legal and regulatory framework for AI-driven banking fraud in India, the United States, and the United Kingdom against four benchmarks: coverage (whether legal definitions capture AI-specific fraud mechanisms), attributability (whether liability can be fixed on a human actor or institution when AI is involved), enforceability (whether investigative and supervisory tools can handle AI-mediated evidence), and proportionality (whether penalties and remedies match the harm AI-enabled fraud causes). Applying these benchmarks to primary law, regulatory instruments, and decided and pending case law, the paper finds that no jurisdiction scores strongly on all four. The United Kingdom leads on coverage and enforceability but is only partial on attributability and proportionality; the United States is strong on enforceability but unsettled on the other three; and India is weak on enforceability and proportionality while, like the United States, untested rather than deficient on coverage and attributability. The paper argues that the binary of a 'reactive' India against 'proactive' Western comparators is misleading: the three jurisdictions are converging on a sectoral, regulator-led model and differ chiefly in the institutional durability of their rule-making processes, not in the protectiveness of the rules those processes produce.

Keywords: *AI-driven banking fraud; comparative financial regulation; Regulation E; Payment Systems Regulator; Reserve Bank of India; legal transplants; algorithmic accountability; fintech governance*

I. INTRODUCTION

Generative artificial intelligence (AI) has changed how banking fraud is committed before banks' regulatory frameworks have caught up with it. A voice synthesised from a few seconds of public audio, a video call mimicking a bank's fraud-prevention officer, or a synthetic identity assembled from data scraped across the internet can now defraud a customer or open a mule account at a speed and scale that conventional deception could not match. AI can feature in banking fraud in three distinct ways: *AI-enabled* fraud, where AI facilitates an otherwise conventional fraud, such as an AI-generated phishing message; *AI-instrument* fraud, where the fake is itself an AI creation and the basis of the fraud, as in synthetic-identity documentation or real-time



deepfake impersonation; and *AI-accelerant* fraud, where AI scales a conventional fraud in speed or volume, as in credential stuffing or transaction layering. This typology does not track any single jurisdiction's legal categories; it is the factual baseline against which this paper tests whether Indian, American, and British law has been drafted or adapted for AI-driven fraud in any of these forms.

The three jurisdictions are naturally comparable because they represent three different approaches to AI-related conduct in financial services. India relies on general cyber and data-protection statutes supplemented by Reserve Bank of India (RBI) circulars, adapting reactively rather than proactively. The United States has a federal statutory system whose provisions have largely been elaborated through litigation. The United Kingdom's conduct regulator is principles-based but holds binding rule-making powers, while a separate statutory reimbursement scheme targets authorised-push-payment fraud specifically. This spread mirrors the absence of any dominant regulatory template in cross-jurisdictional surveys of AI regulation in finance (Crisanto et al., 2024).

A recurring theme in policy and academic debate is whether India's approach to AI-driven banking fraud lags behind more proactive, regulator-led models in the United States and the United Kingdom. This paper examines the doctrinal evidence and concludes that the claim must be qualified once the comparison is disaggregated into separate functional benchmarks rather than treated as a single binary judgment.

Banking supplies the organising context because the proceeds of almost any fraud pass through banks, and banking is among the most heavily regulated sectors in all three jurisdictions; if AI-driven fraud is inadequately addressed here, it is likely inadequately addressed elsewhere. The analysis is limited to retail and commercial banking, noting where each jurisdiction draws the line between banks and non-bank payment providers differently. Part II sets out the four benchmarks, Part III applies them jurisdiction by jurisdiction, Part IV compares the three and draws out recurring patterns, and Part V concludes.

II. RESEARCH METHODOLOGY

Comparing Indian, American, and British law provision by provision is of limited value, since the three systems use different terminology and rest on different institutional frameworks. India's Information Technology Act and Digital Personal Data Protection Act sit alongside RBI circulars that bind as a regulatory regime rather than as primary legislation; the United States divides the subject between a consumer-protection statute administered substantially through litigation, an anti-money-laundering regime, and guidance from an independent consumer-protection agency; and the United Kingdom relies on a conduct regulator's rulebook, a stand-alone criminal statute, and a dedicated reimbursement scheme. Matching these instruments by form would overlook functionally equivalent protections housed in differently shaped instruments.

This paper therefore adopts the functional approach to comparative law associated with Zweigert and Kötz (1998, pp. 34–36). It asks not whether two jurisdictions have 'the same law', but what function a rule serves, and then looks for the rule, whatever its form, that performs that function elsewhere. Five functions are



examined: defining the conduct as fraud, placing a duty of care on financial institutions, allocating liability between institution and customer when that duty is breached, giving the victim a route to redress, and giving the regulator or prosecutor practical tools to enforce. Primary legislation, a regulator's binding rule, and a central bank's circular can thus be read on the same analytical footing.

The functional reading is organised around four benchmarks. **Coverage** asks whether statutory or regulatory definitions are broad enough to capture AI-specific fraud mechanisms or remain bound by pre-AI typologies. **Attributability** asks whether, where an AI system is involved, liability can meaningfully be fixed on a human actor or institution, whether the fraudster used AI as a weapon or the bank used AI as its own opaque or transparent system. **Enforceability** asks whether investigative and prosecutorial tools are sufficient for AI-mediated evidence, including digital-forensics capacity and any obligation on a regulated entity to provide explainability. **Proportionality** asks whether penalties, reimbursement requirements, and regulatory actions are proportionate to the scale and sophistication of AI-driven fraud rather than to a single, manually committed offence.

Within each jurisdiction, primary legislation is treated as authoritative on coverage, regulatory instruments on enforceability, and judicial decisions, where they exist, on attributability. The benchmarks are deliberately not combined into a composite score: robust enforcement is of no help to a victim whose conduct falls outside any covered offence. The material examined is limited to primary legislation, regulatory instruments, and reported or filed case law as of the date indicated for each source, supported by secondary academic and institutional commentary.

III. RESULTS

A. India

India's response to AI-driven banking fraud rests largely on statutes not drafted with AI in view. The Information Technology Act, 2000 remains the principal cyber-law statute for banking fraud committed through a computer system: section 66C penalises identity theft, and section 66D penalises cheating by personation using a computer resource (Information Technology Act, 2000, ss. 66C–66D). Both provisions were written when impersonation meant misusing a stolen password, not a generative model synthesising a victim's voice or likeness. Whether the 'unique identification feature' in section 66C extends to an AI-generated biometric or behavioural signature, and whether 'personation' in section 66D encompasses a deepfake video or audio call, is unanswered by the text and unresolved in any reported Indian decision.

The Digital Personal Data Protection Act, 2023 governs the collection and processing of the personal data on which both AI-powered fraud and AI-powered fraud detection rely, but it was framed around conventional data-processing relationships and does not explicitly address data scraped from public sources to train an impersonation model (Digital Personal Data Protection Act, 2023). General criminal law, principally the offences of cheating and forgery in the Bharatiya Nyaya Sanhita, 2023 (ss. 318, 336), supplies residual,



technology-neutral cover, but its sentencing regime and rules of evidence were designed for a single victim deceived manually, not for an automated pipeline capable of defrauding thousands simultaneously.

The substantive detail of India's fraud-prevention obligations lies in the RBI's Master Direction on Digital Payment Security Controls, which requires regulated entities to 'document and implement the configuration aspects for identifying suspicious transactional behaviour' and provides that 'system alerts shall be parameterised and monitored', for instance by transaction velocity and geo-location anomalies (Reserve Bank of India [RBI], 2021a, paras. 36–37). It does not name AI, but its technology-neutral, outcome-based drafting extends automatically to AI-based monitoring systems, a coverage advantage; it does not, however, require a regulated entity to explain a particular decision, an attributability and enforceability limitation. The RBI's zero and limited liability framework allocates loss according to customer or bank negligence (RBI, 2017), but it predates AI-enabled social engineering at scale and does not distinguish between an 'unauthorised' and an 'authorised but induced' transaction with AI in mind. The Integrated Ombudsman Scheme and the CERT-In incident-reporting directions add, respectively, a dispute-resolution and an incident-reporting layer, both technology-neutral and neither requiring a complaint or report to be flagged as AI-mediated (Ministry of Electronics and Information Technology, 2022; RBI, 2021b).

India's most recent engagement with AI is the report of the Committee on the Framework for Responsible and Ethical Enablement of Artificial Intelligence (FREE-AI), submitted in August 2025, which sets out seven guiding principles and twenty-six recommendations, including a graded-liability and supervisory framework and amendments to seven existing Master Directions to bring AI expressly within their scope (RBI, 2025). None of the recommendations has yet been converted into a binding Master Direction, so the report remains a roadmap rather than an operative instrument. India has no AI-specific statute, and its framework is better described as sectoral than as absent, resembling the United Kingdom's model discussed in Part III.C and differing mainly in institutional development rather than design.

Measured against the four benchmarks, India's coverage is plausible but untested, since its core offence definitions predate AI-related fraud mechanisms; attributability is unaddressed by the liability circulars; enforceability is weak, since the only route is to contest a decision after the fact; and proportionality is broadly reactive, since the liability framework was built for conventional, not AI-accelerated, fraud.

B. The United States

The principal federal consumer-protection law for unauthorised electronic fund transfers is the Electronic Fund Transfer Act, implemented through Regulation E (Electronic Fund Transfer Act, 1978). Its coverage of AI-driven fraud turns on the definition of an unauthorised transfer, which excludes a transfer by a person to whom the consumer furnished the means of access. Where a consumer is tricked by AI into initiating a transfer personally, rather than handing a fraudster access, the transfer may fall outside the Act's protection, a question now being actively litigated.



The Bank Secrecy Act requires financial institutions to maintain anti-money-laundering programmes and file suspicious-activity reports (Bank Secrecy Act, 1970), often through the same machine-learning monitoring systems whose explainability is contested elsewhere in this paper. The Dodd-Frank Act's prohibition on unfair, deceptive, or abusive acts or practices (UDAAP), enforced by the Consumer Financial Protection Bureau (CFPB), is in principle the most flexible American instrument, capable of reaching an institution's failure to prevent AI-powered fraud even where the payment network falls outside the Electronic Fund Transfer Act (Dodd-Frank Wall Street Reform and Consumer Protection Act, 2010, § 1031).

The federal prudential regulators (the Federal Reserve, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation) apply interagency model-risk-management guidance setting standards for model development, validation, monitoring, and governance (Board of Governors of the Federal Reserve System & Office of the Comptroller of the Currency, 2011; Federal Deposit Insurance Corporation, 2017). Although it predates generative AI and does not name it, the guidance is technology-neutral and reaches AI and machine-learning models, including fraud-detection systems. This supplies an enforcement tool largely absent in India: an audit of an institution's AI-based fraud-detection system for its own soundness, not merely for the results it produces.

The clearest example of the American model's reliance on litigation is the New York Attorney General's action against Citibank, alleging inadequate controls against online fraud that led to unreimbursed customer losses through wire transfers. In January 2025 the district court denied Citibank's motion to dismiss, rejecting the argument that the Act categorically excludes consumer wire transfers, and certified the ruling for interlocutory appeal; whether the Act reaches such fraud-induced transfers is now a question of first impression before the Second Circuit (*People of the State of New York v. Citibank, N.A.*, 2025). A parallel example is the CFPB's December 2024 action against Zelle operator Early Warning Services and three of its bank owners, alleging inadequate fraud protection and unlawful denial of reimbursement, which the Bureau voluntarily dismissed on 4 March 2025 after a change in leadership (*Consumer Financial Protection Bureau v. Early Warning Services, LLC*, 2025). The dismissal illustrates the vulnerability of litigation-dependent consumer protection: when an agency's appetite for litigation weakens, the elaboration of substantive law can stall entirely.

Similar volatility exists at state level. In May 2024 Colorado enacted the first comprehensive state AI statute, imposing duty-of-care and impact-assessment requirements on developers and deployers of high-risk AI systems in sectors including financial services; its effective date was postponed to June 2026; in April 2026, after a constitutional challenge, the state attorney general agreed in a stipulated federal court order not to enforce it pending a ruling on a preliminary injunction; and on 14 May 2026 the governor signed a replacement statute repealing the core obligations in favour of a narrower disclosure regime effective January 2027 (Colorado Senate Bill 24-205, 2024; Colorado Senate Bill 26-189, 2026). No version of the statute was in force during the period reviewed.



Measured against the four benchmarks, the American approach is broader than India's on coverage in principle but contested in the Citibank litigation; attributability remains unsettled after the Zelle dismissal, with Citibank the surviving test; enforceability is comparatively strong, resting on prudential model-risk-management infrastructure; and proportionality is as unresolved as it was before the Zelle litigation was filed.

C. The United Kingdom

The Fraud Act 2006 creates the general offence of fraud, including fraud by false representation, and an offence of making, adapting, or supplying articles for use in fraud (Fraud Act 2006, ss. 2, 7). The latter offence proved sufficient, without amendment, to convict the operator of a subscription platform that let criminals spoof bank caller ID and harvest PINs and one-time passcodes, after police found that more than 200,000 people in the United Kingdom had been targeted through it (*R v Fletcher*, 2023), showing that general fraud provisions can reach AI-adjacent fraud infrastructure. English statutory interpretation also offers the clearest doctrinal basis of the three jurisdictions for reading an older provision to reach new technology: the 'always speaking' principle, under which a statute is read as accommodating later developments provided its original purpose can still sensibly be applied (*R (Quintavalle) v Secretary of State for Health*, 2003, para. 9).

The core protection of the Payment Services Regulations 2017 attaches to unauthorised payments; an AI-driven social-engineering fraud that induces the customer's own authorisation falls outside it (Payment Services Regulations 2017). The Financial Conduct Authority's (FCA) Systems and Controls sourcebook requires firms to maintain adequate financial-crime controls (FCA, n.d.-b); it is technology-neutral and applies to AI-based fraud-detection systems, but does not compel a firm to give reasons for a specific automated decision. Separately, because the cross-sectoral Consumer Duty is drafted around outcomes, a firm's failure to update its fraud-detection systems for a changing typology such as AI-enabled social engineering could in principle itself breach the Duty (FCA, n.d.-a; Financial Services and Markets Act 2023).

A distinctive feature of the British framework is the mandatory reimbursement scheme for authorised push payment fraud, in force since October 2024, which requires in-scope payment service providers to reimburse victims up to £85,000 per claim, usually splitting the cost equally between sending and receiving institutions (Payment Systems Regulator [PSR], 2023, paras. 3.45–3.52). Unlike the Indian and American regimes, which rely on general rules for unauthorised transactions, the British scheme imposes bespoke liability for precisely the fraud AI social engineering is designed to trigger, authorised but induced payments, though its monetary cap and its exclusion of international transfers, a preferred route for cross-border fraud, limit that protection. The main legal limits of the framework were set in *Philipp v Barclays Bank UK plc* (2023), where the claimant had been deceived by fraudsters posing as law-enforcement officers into instructing Barclays to transfer funds abroad. The Supreme Court unanimously held that the *Quincecare* duty, a bank's duty not to execute an instruction it has reasonable grounds to suspect is an attempt to misappropriate the customer's money (*Barclays Bank plc v Quincecare Ltd*, 1992), does not apply where the customer personally gives the



instruction, even if deceived. AI-enabled social engineering is designed precisely to produce such a technically valid instruction, so *Philipp* narrows attributability exactly where AI-driven fraud is most active, leaving the statutory reimbursement scheme as the victim's main remedy.

The Bank of England and the FCA have not issued a single landmark report on AI in banking but have worked together on a sustained basis, publishing a joint discussion paper on AI and machine learning (DP5/22) as early as October 2022 and regularly surveying AI adoption and its risks, giving both regulators a current evidential basis for supervisory action (Bank of England & Financial Conduct Authority, 2022). Measured against the four benchmarks, the British framework shows functional coverage through general fraud provisions; attributability narrowed by the common law, with statutory reimbursement substituted as the main remedy; comparatively strong enforceability through FCA and PSR supervisory powers; and proportionality that is qualified rather than complete, since the reimbursement scheme is capped and excludes international transfers.

D. Comparative Synthesis

The qualitative ratings are summarised in Table 1. 'Strong' means the benchmark's objective is met through a binding precedent or an operative instrument in force; 'Partial' means it is met through a qualified path, for instance one subject to a monetary cap, a narrowing judicial decision, or dependence on institutional continuity; and 'Weak' means no demonstrated path to the objective exists.

Table 1: Four-benchmark comparative synthesis

Benchmark	India	USA	UK
Coverage	Partial: plausible but untested	Partial: contested in litigation	Strong: demonstrated in prosecution
Attributability	Weak: unaddressed by circulars	Partial: actively contested	Partial: narrowed by <i>Philipp</i>
Enforceability	Weak: outcome-only supervision	Strong: model-risk-management infrastructure	Strong: FCA/PSR supervisory powers
Proportionality	Weak: general liability rules	Weak: general and contested	Partial: bespoke but capped scheme

Source: Author's qualitative synthesis derived from the doctrinal analysis in Part III.

No jurisdiction rates strong across all four benchmarks. The United Kingdom performs best on coverage and enforceability but only partially on attributability and proportionality. The United States is strong only on



enforceability, with the other three benchmarks unsettled or contested. India is weak on enforceability and proportionality while remaining, like the United States, doctrinally untested rather than definitively weak on coverage and attributability.

IV. DISCUSSION

A. Reading the Benchmarks Together

Though conceptually distinct, the four benchmarks interact in practice. Applying them to a common hypothetical, a customer misled by an AI-generated deepfake call into authorising a payment with their own banking credentials, reveals three recurring patterns, consistent with academic literature on automated financial-crime monitoring that treats explainability and due process as live rather than settled issues (Turksen et al., 2024).

The first pattern, most evident in India, is *compounding uncertainty*. Where coverage, attributability, and enforceability are all unsettled at once, the victim faces three open questions in succession, each of which must be resolved favourably before redress is available. Whether the conduct falls within section 66D, whether the transaction falls under the zero- or limited-liability circular, and whether the bank's AI-based monitoring system failed the Master Direction's outcome-based standard are each, independently, open questions.

The second pattern, most visible in the United Kingdom, is *compensating substitution*. Where one benchmark works against the victim, as with the narrow common-law attributability after *Philipp*, another may work in their favour, here the PSR's reimbursement scheme on proportionality. This resilience is not protectiveness: the United Kingdom's position is better characterised as predictable than as favourable to the victim.

The third pattern, most prominent in the United States, is *contingency on institutional continuity*. Enforceability, and with it attributability, depends on an enforcement agency's litigation posture, so a strong position can weaken without any legislative change, simply through a change in political leadership. The Indian and British frameworks, whose central bank and conduct regulator issue binding rules through processes less exposed to a single change in leadership, do not share this volatility to the extent the Zelle sequence demonstrates in the United States.

B. Revisiting the 'Reactive India, Proactive Comparators' Claim

A common observation in comparative analysis is that Indian law is reactive compared with American and British law. The evidence in Part III both supports and qualifies this. It supports the characterisation on enforceability and proportionality: the RBI's supervisory instruments focus on outcomes rather than process, and the liability circulars did not anticipate the volume of fraud AI enables, unlike the model-risk-management and systems-and-controls approaches of the American and British frameworks.

On coverage and attributability, however, the picture is less one of Indian reactivity than of all three jurisdictions being unsettled. The United States has not resolved attributability any more definitively than



India; it has moved the question into live litigation, a fragile path, as the Zelle dismissal shows. The United Kingdom's apparently final answer in *Philipp* narrows protection rather than expanding it. 'Reactive' therefore aptly describes India's enforceability and proportionality framework, but only incompletely its coverage and attributability framework, which is better described as untested than absent.

On this evidence, the more accurate difference among the three jurisdictions lies not in the protectiveness of the rules their processes have produced, but in the institutional durability of those processes, a difference that points toward convergence on a sectoral, regulator-led approach. This is independently confirmed by an OECD survey of forty-nine jurisdictions, which finds that most are applying existing, technology-neutral financial regulation supplemented by AI-specific guidance rather than creating AI-specific financial regulation (OECD, 2024).

C. Transferability

Three elements of the comparator frameworks appear transferable to India. First, American supervisory model-risk-management guidance, which examines the soundness of an institution's AI-based fraud-detection system and not merely its results, requires no new primary legislation and could become a further RBI Master Direction; the FREE-AI committee's recommendation to revise seven existing Master Directions suggests the RBI is already moving in that direction. Second, the British bespoke reimbursement scheme for authorised-but-induced payment fraud addresses India's proportionality gap more directly than extending the existing liability circulars would, though it would need calibration to Indian payment limits and cross-border coverage. Third, more speculatively, the Bank of England and FCA practice of joint supervisory surveys offers a durable, evidence-based supervisory model independent of litigation.

This analysis rests on Watson's (1993, pp. 21–30) account of legal transplants rather than Legrand's (1997) rival account, which treats a rule's meaning as inseparable from its host jurisdiction's interpretive culture. The three elements identified are regulatory instruments, not judge-made doctrine, so their meaning depends more on the instrument's text and the regulator's technical capacity than on interpretive culture, closer to Watson's portable conception than to Legrand's embedded one.

Two limits should be noted. First, none of the three elements addresses coverage; all operate on enforceability or proportionality, leaving untouched the more fundamental question of whether sections 66C and 66D reach AI-generated impersonation, which only judicial interpretation or statutory amendment can resolve. Second, transferability in this sense is not the same as political, administrative, or fiscal feasibility, which lies outside this paper's doctrinal method.

D. Limitations

Three limitations should be stated. First, the law in this field shifts quickly, as the FREE-AI report and the Colorado repeal and replacement illustrate, so any claim about the 'current' position is time-bound. Second,



the comparative claims are bounded by the four benchmarks chosen; benchmarks grounded in other concepts, such as compliance cost to regulated entities rather than protection of victims, might yield a different ranking. Third, the functional method can identify a definitional gap, an unaddressed doctrinal question, or an absent supervisory tool, but cannot by itself establish that a particular gap has caused particular victims harm, an empirical question beyond this paper's scope.

V. CONCLUSION

This paper has mapped the legal and regulatory regime governing AI-driven banking fraud in India, the United States, and the United Kingdom and assessed it functionally against four benchmarks: coverage, attributability, enforceability, and proportionality. In all three jurisdictions, general cyber and data-protection law is supplemented by sector-specific instruments: in India, by RBI circulars and, since August 2025, a detailed but non-binding committee report; in the United Kingdom, by conduct regulation, a statutory reimbursement scheme, and a rolling joint-supervisory programme. None performs every function well.

The United Kingdom ranks first on coverage and enforceability but is only partial on attributability, given *Philipp*'s narrowing effect, and limited on proportionality by its capped scheme. The United States is comparatively strong on prudential enforcement infrastructure but has resolved neither coverage nor attributability, and its litigation-driven model has proved susceptible to enforcement-agency discontinuity. India trails on enforceability and proportionality, though the FREE-AI report suggests movement toward the American and British models, and remains, like the United States, untested rather than definitively deficient on coverage and attributability.

Three findings stand out. First, rather than diverging, the three jurisdictions are converging on a broadly sectoral, regulator-led model, a convergence the 'reactive India, proactive comparators' framing underplays. Second, legal protectiveness is analytically distinct from institutional durability: *Philipp* is durable but narrowing, while the American litigation-driven model is potentially protective but institutionally fragile, so neither offers an unqualified model for transplantation. Third, on current evidence, enforceability rather than coverage most clearly marks India's gap relative to its comparators, and is where reform might most plausibly begin, through the mechanism the FREE-AI report already gestures toward: placing on the regulated entity the burden, if challenged, of showing that a decision by its automated fraud-detection system was appropriate in the circumstances.

Finally, the pace at which this ground is shifting is itself a finding: the comparison is a snapshot rather than an endpoint, which reinforces the case for a functional method that reads each jurisdiction's instruments for the function they perform rather than their current form.



REFERENCES

- Bank of England & Financial Conduct Authority. (2022). *Artificial intelligence and machine learning* (Discussion Paper DP5/22). Bank of England.
- Bank Secrecy Act, 31 U.S.C. § 5311 et seq. (1970).
- Barclays Bank plc v Quincecare Ltd [1992] 4 All ER 363 (QB).
- Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023 (India).
- Board of Governors of the Federal Reserve System & Office of the Comptroller of the Currency. (2011). *Supervisory guidance on model risk management* (SR Letter 11-7; OCC Bulletin 2011-12).
- Colorado Senate Bill 24-205, Consumer Protections for Artificial Intelligence (2024) (as amended by Senate Bill 25B-004).
- Colorado Senate Bill 26-189, An Act Concerning Automated Decision-Making Technology (2026) (effective January 1, 2027).
- Consumer Financial Protection Bureau v. Early Warning Services, LLC, Bank of America, N.A., JPMorgan Chase Bank, N.A., & Wells Fargo Bank, N.A., No. 2:24-cv-03652 (D. Ariz. voluntarily dismissed Mar. 4, 2025).
- Crisanto, J. C., Leuterio, C. B., Prenio, J., & Yong, J. (2024). *Regulating AI in the financial sector: Recent developments and main challenges* (FSI Insights on Policy Implementation No. 63). Bank for International Settlements.
- Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India).
- Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, § 1031, 124 Stat. 1376 (2010) (codified at 12 U.S.C. § 5531).
- Electronic Fund Transfer Act, 15 U.S.C. § 1693 et seq. (1978); Regulation E, 12 C.F.R. pt. 1005.
- Federal Deposit Insurance Corporation. (2017). *Adoption of supervisory guidance on model risk management* (Financial Institution Letter FIL-22-2017).
- Financial Conduct Authority. (n.d.-a). PRIN 2A: The Consumer Duty (in force July 31, 2023). In *FCA Handbook*.
- Financial Conduct Authority. (n.d.-b). SYSC 6.3: Financial crime. In *Senior management arrangements, systems and controls sourcebook, FCA Handbook*.
- Financial Services and Markets Act 2023, c. 29 (UK).
- Fraud Act 2006, c. 35 (UK).
- Information Technology Act, 2000, No. 21 of 2000 (India).
- Legrand, P. (1997). The impossibility of 'legal transplants'. *Maastricht Journal of European and Comparative Law*, 4(2), 111–124.



- Ministry of Electronics and Information Technology. (2022). *Cyber security directions under section 70B(6) of the Information Technology Act, 2000* (No. 20(3)/2022-CERT-In). Government of India.
- OECD. (2024). *Regulatory approaches to artificial intelligence in finance* (OECD Artificial Intelligence Papers). OECD Publishing.
- Payment Services Regulations 2017, SI 2017/752 (UK).
- Payment Systems Regulator. (2023). *Fighting authorised push payment fraud: A new reimbursement requirement* (Policy Statement PS23/3).
- People of the State of New York v. Citibank, N.A., No. 1:24-cv-00659 (S.D.N.Y. Jan. 2025) (order denying motion to dismiss), interlocutory appeal pending (2d Cir.).
- Philipp v Barclays Bank UK plc [2023] UKSC 25.
- R (Quintavalle) v Secretary of State for Health [2003] UKHL 13.
- R v Fletcher (Southwark Crown Court, May 19, 2023) (unreported; sentencing remarks of HHJ Sally Cahill KC).
- Reserve Bank of India. (2017). *Customer protection – Limiting liability of customers in unauthorised electronic banking transactions* (RBI/2017-18/15, DBR.No.Leg.BC.78/09.07.005/2017-18).
- Reserve Bank of India. (2021a). *Master direction on digital payment security controls* (RBI/2020-21/74).
- Reserve Bank of India. (2021b). *Reserve Bank – Integrated Ombudsman Scheme, 2021* (RBI/2021-2022/101).
- Reserve Bank of India. (2025). *Framework for responsible and ethical enablement of artificial intelligence (FREE-AI): Report of the committee*.
- Turksen, U., Benson, V., & Adamyk, B. (2024). Legal implications of automated suspicious transaction monitoring: Enhancing integrity of AI. *Journal of Banking Regulation*, 25(4), 359–377. <https://doi.org/10.1057/s41261-024-00233-2>
- Watson, A. (1993). *Legal transplants: An approach to comparative law* (2nd ed.). University of Georgia Press.
- Zweigert, K., & Kötz, H. (1998). *An introduction to comparative law* (T. Weir, Trans.; 3rd ed.). Oxford University Press.