Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue S1,* 2026
Gurugram University Conference : 09-10 April 2026
Website: https://ceapress.org

The Invisible Thread of Risk: Balancing Convenience and Security on Mobile Banking Platforms

Hitika Singh[1]*, Anmol Arora[2], Dr. Myunghoon Roh[3]
Ph.D. Scholar, Department of Law,
Gurugram University

Submission date 12.04.2026 | Acceptance date: 25.04.2026 | Publication: 29.05.2026

ABSTRACT

Mobile banking has also brought a dynamic change in the way we deal with our personal finances, making it less hassling and convenient. However, there is a threat implicit with this facility since mobile banking projects are more vulnerable to cyberbanking and economic crime respectively. The paper is related to the trade-off of functionality and safety in mobile banking systems. The threats are increasing and they are becoming a big threat to users. With the increasing popularity of mobile banking, cyber threats, including phishing, malware, and identity theft, have become more prevalent. Such weaknesses not only compromise confidential data of clients but also cast doubt on the security of mobile banking applications. Also, the fact that mobile service platforms are diverse and the user is not aware of how to effectively protect his/her devices will contribute to the issue. The analysis determines the existing state of mobile banking security and ultimately concludes that it leaves much to be desired and is posing a grave danger to the security of the users. It also discusses the ways financial institutions, regulators, and technology vendors can reduce these risks. The paper describes the multidimensional approach to the balancing of convenience and security with a strong level of security, user education and legal environments that motivate citizens to use it in a safe manner. This exploration has very significant implications on the future of smartphone banking and the significance of collaborative problem solving towards the future of smartphone banking in the midst of growing risk and challenges. By addressing the invisible thread of risk that is knitted in mobile banking we can make the cellular financial environment much more favorable to users, stakeholders and regulating agencies.

Keywords: *Mobile banking, financial fraud, Cyber threats, User awareness, Regulatory frameworks.*

Introduction

The invention of mobile banking systems has brought a revolution in the financial services industry and allowed consumers all over the world more convenience and the possibility to

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue S1,* 2026
Gurugram University Conference : 09-10 April 2026
Website: https://ceapress.org

access financial services than ever.[1] However, with this digital transformation, there are intricate cybersecurity risks, growing fears about privacy, and novel risks posed by user behaviour.[2] Mobile banking has joined the financial transactions that people engage in everyday and it is worthy that these platforms are regulated and secured. In this report we attempt to assess the present situation of regulation of mobile banking in terms of cybersecurity. We consider risks through the lens of privacy and through the lens of privacy of user behaviour and discuss the potential way to achieve a more beneficial balance between convenience and security. Mobile banking platforms are at the cross-section of technological innovation and financial regulation.[3] There has been an increase in cyber-attacks in the last few months that involve phishing, malware and social engineering based on technical and human vulnerabilities due to the breakneck pace of the adoption of these platforms in the past few months.[4] In reaction, a number of regulations established frameworks, guidelines and supervisory practices to curb such risks.[5] However, the threats nature continuously varies, the user requirements constantly evolve, and new technologies continue to be incorporated (AI and ML, in particular).[6] In this report the results of recent studies are pooled together in order to evaluate the advantages and disadvantages of the existing forms of regulation and put forward a case of new forms of regulation that would provide a greater balance between user convenience and security.

Digitalization has transformed the way financial services operate today.[7] Mobile banking platforms have emerged as a key component of the new global banking stack. Recent advances in smartphone technology and higher rate of internet penetration have made mobile banking possible. There is increased fintech creativity that is appealing to tech-savvy users who can conveniently perform a variety of financial transactions from their mobile phones at any time and from any location.[8] This paradigm shift has not only improved financial inclusion and customer experience mostly but also exposed banking systems and users to multi-layered cybersecurity, data privacy and user behaviour risk.[9] With the introduction of mobile banking platforms, it has transformed the finance sector, and customers are given unique user access on a global scale. It also means that the digital transformation has brought along complicated cyber-attacks, increased privacy issues and changing user behaviour. With mobile banking being central to so much of our financial activity, it seems critical that regulatory strategies be able to protect these platforms from bad actors. This report examines the effectiveness of current regulation in managing the

[1] Shaikh AA and Karjaluoto H, 'Mobile Banking Adoption: A Literature Review' (2015) 32 *Telematics and Informatics* 129.

[2] Organisation for Economic Co-operation and Development (OECD), *Digital Security Risk Management for Economic and Social Prosperity* (OECD Publishing 2015).

[3] Douglas W Arner, Janos Barberis and Ross P Buckley, 'The Evolution of Fintech' (2016) 37 *Northwestern Journal of International Law and Business* 127.

[4] Verizon, *2025 Data Breach Investigations Report* (Verizon 2025).

[5] Reserve Bank of India, *Master Direction on Digital Payment Security Controls* (RBI 2021).

[6] Financial Stability Board, *The Financial Stability Implications of Artificial Intelligence* (FSB 2024).

[7] World Bank, *The Global Findex Database 2021* (World Bank 2022).

[8] International Telecommunication Union, *Measuring Digital Development: Facts and Figures 2024* (ITU 2024).

[9] Basel Committee on Banking Supervision, *Principles for Operational Resilience* (Bank for International Settlements 2021).

risks of cybersecurity, privacy and user behaviour in the context of rapidly evolving mobile banking technologies. It also sets out new strategies that could be adopted to help consumers and businesses balance the conflict between convenience and security. Mobile banking platforms are operating at the crossroad of two radically different worlds, that of the fast pace of technological development and that of the heavy regulation of finance, where technology often outpaces the development of law and supervision. The proliferation of these platforms has been accompanied by an exponential increase in the number and sophistication of cyber threats (including phishing attacks, malware intrusions, identity thefts and social engineering schemes), many of which prey not only on system vulnerabilities but also on human behavioural patterns.[10] In this context, user behaviour - poor password practice, vulnerability to phishing communications and low levels of cyber awareness – has become an important risk factor that traditional regulatory approaches have found difficult to address effectively.[11]

In this regard, regulatory bodies in various jurisdictions have reacted by devising legal frameworks, rules and compliance mechanisms for increasing the resilience of cybersecurity and safeguarding data received from users.[12] However, the performance of these regulatory frameworks in this domain is patchy and intertwined with issues such as regulatory fragmentation, inefficiency or lack of harmonization and enforcement bottlenecks while cyberthreats continue to evolve at a rapid pace.[13] Additionally, the use of new technologies in mobile banking ecosystems such as artificial intelligence (AI), machine learning (ML) and biometric authentication presents further regulatory challenges related to algorithmic accountability, data governance and ethics of technology.[14] In this context, there is an urgent need to carefully assess whether the existing regulatory frameworks are sufficient to address the interlinked problems of cyber threats, privacy risks and user behaviour risks. Thus, there is a lack of empirical evidence on the status quo of current data regulatory strategies, their main pitfalls and potential solutions for new efficient regulatory frameworks that are adaptive, technology-neutral and user-centric. This study thus highlights the need for a multi-faceted safeguarding regulatory model of mobile banking technology, which amalgamates technological safeguards, legal measures and behavioural analytics to foster a secure, resilient and trusted mobile payment ecosystem.

Cybersecurity Threats: Regulatory Strategies and Outcomes

Phishing and malware are some of the most common security threats that can threaten mobile banking platforms.[15] Phishing, for example, remains a persistent threat that exploits both

[10] Europol, *Internet Organised Crime Threat Assessment 2024* (Europol 2024).
[11] Lorrie Faith Cranor, *Security and Usability: Designing Secure Systems That People Can Use* (O'Reilly Media 2005).
[12] European Banking Authority, *Guidelines on ICT and Security Risk Management* (EBA 2019).
[13] World Economic Forum, *Global Cybersecurity Outlook 2025* (WEF 2025).
[14] Johnson Kh and others, 'Artificial Intelligence in Banking: Ethical and Regulatory Challenges' (2023) 18 *Journal of Financial Regulation and Compliance* 201.
[15] APWG, *Phishing Activity Trends Report* (Anti-Phishing Working Group 2024).

technology weaknesses and human behaviour to steal sensitive data. One popular countermeasure today that is not implemented or effective at all institution sites is multi-factor authentication (MFA).[16] An advanced cyber security framework is considered best practice for financial institutions, but the level of supervision and harmonization from regulation varies widely between jurisdictions.[17] Regulatory regimes to address cyber threats in the mobile banking environment are less concerned with creating an economic incentive framework and more concerned with deploying certain technical controls such as multi-factor authentication, encryption and secure-coding practices. MFA is considered an effective defense against unauthorized access and credential compromise. The methods were observed to be very common in online banking. The strength and usability of MFA implementations differ widely, including institutions that utilize some relatively less impactful types such as SMS-based codes that are easily intercepted. More sophisticated MFA methods add additional security, like biometric and graphical password systems, but this comes with a usability cost. Cybersecurity models tailored for financial institutions extend to almost everything, from identification, risk managed frameworks, incident response and continuous monitoring. However, it is necessary not just to have all these frameworks strictly implemented, but to update them on a regular basis to respond to new threats.[18] In reality, however, regulation is employed as an enforcement measure by different jurisdictions, and this results in a highly uneven protection of the sector. Target and controls are done using mouse and human props. One of the barriers that will never be overcome is phishing. The regulatory measures have promoted awareness campaigns and education among users. But phishing has evolved higher and has outsmarted most of the conventional defenses. The point of responsibility of users to be aware is underlined and further versions of br0wse, preferably, should be equipped with more efficient detection and prevention systems.

Privacy Concerns: Regulatory Adequacy and User Perceptions

Mobile banking application users have always been concerned about privacy.[19] Regulatory frameworks like the GDPR in Europe (and similar efforts elsewhere) set baseline data protection requirements.[20] However, the regulations vary in terms of their scope and enforcement, leading to a patchwork of user data protections across platforms and geographies. That said, users are still concerned about data collection and sharing as well as transparency of privacy practices for mobile finance apps.[21] In this respect, privacy regulations such as GDPR have set basic provisions for data protection like user consent, data minimization and breach notification. A content analysis of privacy policies and user concerns in finance mobile apps shows that although

[16] National Institute of Standards and Technology, *Digital Identity Guidelines* (NIST SP 800-63B, 2023).
[17] National Institute of Standards and Technology, *Cybersecurity Framework 2.0* (NIST 2024).
[18] Center for Internet Security, *CIS Critical Security Controls Version 8* (CIS 2021).
[19] Alan F Westin, *Privacy and Freedom* (Atheneum 1967).
[20] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation).
[21] Nora Ni Loideain, *EU Data Privacy Law and Serious Crime* (Oxford University Press 2019).

regulatory frameworks offer a basic level of protection, users are still worried about the use of their data and the transparency with which privacy policies deal with this information. The inconsistent enforcement of privacy regulations varies from platforms to platforms: Some above, some below. Specific concerns raised by the users include the sharing of personal data with third parties, the way this data is used is not clearly communicated. Some of these issues are being addressed by regulatory approaches that include more disclosure and user rights, but there are still gaps in ensuring people are informed and able to control their data.

User Behavior Risks: Regulatory Interventions and Limitations

User behaviour interaction is an important factor affecting the security of mobile banking platforms.[22] Even though the regulatory bodies have taken steps to mitigate the risks, there are still high-risk points such as weak password practices, susceptibility to social engineering and lack of awareness in security features. Security factors such as the design of user interfaces and authentication mechanisms that may influence user compliance have a strong intrinsic influence on risk.[23] Regulatory strategies like to highlight the technical controls but not so much the impact of behaviour on security. User behaviour is the major deciding factor for various security outcomes in mobile banking platforms. Even as regulators do their best to instill security awareness and best practices, there are still many users who will take the easy option, make poor choices around weak passwords or fall prey to social engineering attacks. How security features are designed in mobile banking apps affects user behaviour considerably. Literature review indicates user interaction with security features, such as transparency and understandability of system prompts and usability of authentication devices, as a determinant of compliance and risk reduction. Regulatory approaches have also emphasized technical controls with little role for behavioural approaches. This leaves a lot of gaps in the human side of security incidents.

Supervisory Practices and Regulatory Divergence

Supervisory practices of large banks show significant differences across jurisdictions, especially between the UK and the euro area.[24] This can give rise to regulatory inconsistencies, which may create potential gaps in the application of consistent cybersecurity and privacy requirements. This divergence could heighten systemic risks and complicate cross-border financial regulatory cooperation. Supervisory practices of the largest banks differ significantly between the UK and the euro area. Supervision in the UK is more appropriately principles-based, while that in the euro area has taken a rules approach through the creation of, inter alia, the Single Supervisory Mechanism. Such differences pose a risk of regulatory divergence, which in turn may misalign

[22] Joseph Bonneau and others, 'The Quest to Replace Passwords' (2012 IEEE Symposium on Security and Privacy).
[23] Serge Egelman, Lorrie Faith Cranor and Jason Hong, 'You've Been Warned' (2008) CHI Proceedings 1065.
[24] Kern Alexander, 'Banking Supervision in the United Kingdom and the Euro Area' (2023) 44 *Company Lawyer* 98.

cybersecurity and privacy standards. Such divergence may create systemic risks, especially for cross-border institutions operating in multiple regulatory regimes.

AI and Machine Learning: Regulatory Adaptation

AI and ML have been successfully adopted in one of the areas of mobile banking and it is creating wide regulatory challenges gradually.[25] But these technologies enhance security and fraud detection capabilities, but also bring concerns over transparency, accountability and data privacy. Existing regulatory regimes are being adapted to meet these challenges, but there are still major gaps in the regulation of AI-based decision-making systems. AI and ML are being embedded in mobile banking platforms, promising more secure, fraud-resistant, personalized services. But these technologies also come with issues of transparency, accountability and data privacy which in turn leads to new regulations. The issues are being cemented within the framework of regulation, but little is being done on overseeing the decision-making processes of AI. Regulators have a new priority: to make excusable reference, and suitable rules are being needed.

Impact of Cybersecurity Threats on Adoption and Innovative Security Solutions

Perceptions of cyber security threats and risks have measurable impacts on broad acceptance of subservient channels.[26] Mobile banking platforms with strong security features and regulatory safeguards are more likely to make users switch. On the other hand, newsworthy hacks and weak regulatory action can kill trust, and slow or reverse adoption. The views on cybersecurity risks and perceived adequacy of protocols to mitigate the perceived risk are considerable drivers of user adoption. Systematic literature review shows that users are more likely to adopt mobile banking platforms when they feel that there is strong security and regulation in place. On the contrary, major security incidents and poor responses from regulators can hurt trust and dissuade users. This has resulted in the research of potential alternatives such as graphical passwords, multi-factor authentication schemes, etc. These approaches use easy-to-use authentication methods to fight technical and behavioural vulnerabilities.

[25] World Economic Forum, *The Future of AI in Financial Services* (WEF 2024).

[26] Maruf Hossain and others, 'The Role of Perceived Security in Mobile Banking Adoption' (2019) 57 *International Journal of Bank Marketing* 215.

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue S1,* 2026
Gurugram University Conference : 09-10 April 2026
Website: https://ceapress.org

User Concern	Regulatory Response	Effectiveness (Findings)
Phishing and Social Engineering	User education, MFA	Persistent threat; user vigilance still critical
Data Privacy	GDPR, disclosure requirements	Baseline protections; transparency and enforcement vary
Weak Passwords	Password policies, MFA	Technical controls in place; behavioral risks remain
Data Sharing with Third Parties	Consent requirements, transparency	Improved disclosure; user empowerment still limited
AI-driven Decisions	Evolving guidelines	Oversight and explainability still developing

Fig.1. User concerns and regulatory responses in Mobile Banking

(Source: Compiled by the author from Reserve Bank of India, Report on Trend and Progress of Banking in India 2023-24; Reserve Bank of India, Master Direction on Digital Payment Security Controls 2021; and International Telecommunication Union, Global Cybersecurity Index 2024)

Contextualizing Findings

All these insights combined indicate that although there has been a substantial advancement in the financial regulatory strategies to curb the effects of cyber security, the risks of privacy and user behavior in mobile banking systems, there are numerous constraints that persist.[27] The regulatory frameworks have established the minimum requirements of technical controls and data protection that offers a minimum level of security and privacy.[28] However, the world of threats is evolving at a fast pace and so are the behavior and the need to introduce adoptions within the regulators as well. One of the key issues is that the management of supervisors varies among jurisdictions particularly when it comes to multinationals of the financial institution.[29] However, the risks of the system or non-harmonizing user protection, which can ultimately cause colossal problems in this area, demand a higher quality of harmonization of regulation and cooperation across borders. The introduction of AI and ML in Mobile Banking Platforms: Opportunities and Challenges These technologies can bring new opportunities and challenges to security and user

[27] Basel Committee on Banking Supervision, *Principles for Operational Resilience* (Bank for International Settlements 2021).
[28] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) [2016] OJ L119/1.
[29] Financial Stability Board, *Cyber Incident Reporting: Existing Approaches and Next Steps for Broader Convergence* (FSB 2023).

experience, but also new risks regarding transparency and accountability.[30] Regulations also need to be modified to offer the relevant control of AI driven processes.

Conclusion

Besides regulatory strategies, technical controls, e.g., MFA and cyber security frameworks (NIST CSF, CIS TOP 20) have been established but their implementation, however, is extremely heterogeneous across institutions and jurisdictions.[31] Some relative improvements have been noted but phishing and social engineering has been a significant threat and consequently is motivating the need to have more resilient, automated defenses. Existing rules and regulations are largely focused on the technical controls and at times attribute human factors as the cause of security incidents. Nonetheless, defensive mechanisms that are caused by humans are not subject to regulations to a great extent. More studies should be done to determine and assess salient behavioral interventions. The basic protections provided by privacy rules are not enough since there is inequality in enforcement and openness. Users are still worried about the data gathering, distribution and transparency of privacy.[32] Other areas of inconsistency and potential vulnerability are significant variation in crossover supervisory practice across jurisdictions. Regulatory challenges are related to harmonization of standards and enhanced cross-border co-operation in regulation. Our tone is one of technical controls, yet user behavioral risks, such as bad password habits, and vulnerability to social engineering attacks, are wasting the day's efforts. A major motivator of compliance is user experience with security features As AI and ML increasingly assume control over mobile banking, regulatory standards will have to adapt to find a balance between the need to safeguard consumer data and accountability and transparency.[33] Regulatory differences between jurisdictions, in particular between the UK and the euro area has led to difficulties in the application of cybersecurity and privacy standards on equal footing. Enabling users to be aware and have control over their personal data is still a challenge. User protection should be a key objective of regulatory methods, through incentivized, transparent models of communication and privacy controls easily available. The adoption of AI and ML brings up new regulatory questions related to transparency and accountability. Existing frameworks are still in development but not fully developed Psychological and regulatory factors why customers are increasingly choosing more options as their mobile banking solutions.

The latest regulatory actions have gone a long way towards curbing the cybersecurity threat and privacy risks in mobile banking systems, primarily by introducing file encryption and

[30] Organisation for Economic Co-operation and Development, *OECD Framework for the Classification of AI Systems* (OECD Publishing 2022).
[31] National Institute of Standards and Technology, *Cybersecurity Framework (CSF) 2.0* (US Department of Commerce 2024).
[32] Daniel J Solove, *Understanding Privacy* (Harvard University Press 2008).
[33] European Banking Authority, *Report on Machine Learning for Internal Ratings-Based Models* (EBA 2021).

strengthening data protection laws and controls.[34] However, these measures are not as efficient due to inconsistent enforcement, different regulatory requirements at various jurisdictions and inadequate focus on user behavior risks. New issues with technologies such as AI and ML are emerging, which numerous laws are not yet even beginning to tackle. The regulators must contribute to the appropriate balance between convenience and security, through behavioral interventions, through harmonization of the standards in different jurisdictions and through close regulation of AI-driven processes.

Recommendations

Design and create user awareness programmes and designs that are human-centric to security incidents.[35] Promote more jurisdictional convergence to cut regulatory differences on cybersecurity and privacy standards.[36] Formulation of explicit guidelines in the application of AI and ML in mobile banking with transparency, explainability and accountability have explicit and easy to understand privacy policies and improved consent and data management systems that allow the users greater control over their personal information.[3738] Encourage and encourage the use of modern security methods which are easy to use like graphical password and biometric security that offer a greater protection without compromising on usability.[39] These areas can be better tackled through regulatory strategies to enhance efficiency in dealing with these areas to combat cybersecurity risks, ensuring user privacy and averting threats of unwanted behavior and ensuring more people use the mobile banking platforms.

The banking sector should use privacy and security by design principles throughout the application's mobile banking lifespan, ranging from developing applications to distribution and support.[40] Continuous assessments of vulnerabilities, testing for penetration, and third-party security audits are necessary to uncover holes before they are exploited by fraudulent individuals. Banks should employ dynamic identification systems that analyze transaction context, device

[34] Reserve Bank of India, *Master Direction on Digital Payment Security Controls* (RBI, 18 February 2021).
[35] M Lynne Markus and Daniel Silverman, 'A Foundation for the Study of IT Effects: A New Look at DeSanctis and Poole's Concepts of Structural Features and Spirit' (2008) 32 Journal of the Association for Information Systems 609.
[36] International Organization for Standardization, ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems.
[37] Finale Doshi-Velez and Been Kim, 'Towards a Rigorous Science of Interpretable Machine Learning' (2017) arXiv preprint arXiv:1702.08608.
[38] Daniel J Solove, 'Privacy Self-Management and the Consent Dilemma' (2013) 126 Harvard Law Review 1880.
[39] Karen Renaud and Judith Ramsay, 'Now What Was That Password Again? A More Flexible Way of Identifying and Authenticating Our Seniors' (2007) 23 Behaviour & Information Technology 369.
[40] Ann Cavoukian, 'Privacy by Design: The 7 Foundational Principles' (Information and Privacy Commissioner of Ontario, 2011).

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue S1,* 2026
Gurugram University Conference : 09-10 April 2026
Website: https://ceapress.org

behaviour, and location-based trends to detect suspicious activity in real time.[41] Regulators may mandate institutions to implement incident response and breach reporting processes for prompt disclosure to consumers and supervisory authorities.[42] Cross-border collaboration among financial regulatory agencies, security authorities, and cybersecurity organizations should be increased to improve information sharing and enforcement methods. To ensure prompt reimbursement for unlawful payments and information breaches, online consumer complaint dispute resolution procedures need to be streamlined and incorporated with ombudsmen procedures.[43] Additionally, vulnerable users, such as the elderly and first-time online financial consumers, should be protected with language specific instructions and accessibility-focused security measures. Banks ought to also keep transparent modeling governance arrangements that detail the certification program, verification, and oversight of artificial intelligence programs utilized for identifying fraudulent transactions and credit decision-making.[44] Conducting ethical impact evaluations and algorithmic audits on a regular basis can reduce discrimination and promote responsible innovation. Ultimately, educational organizations, governing bodies, monetary institutions, and suppliers of technology should work together to create evidence-based standards that strike a balance between innovation, customer convenience, and strong cybersecurity measures in mobile banking platforms.[45]

References

1. Shaikh AA and Karjaluoto H, 'Mobile Banking Adoption: A Literature Review' (2015) 32 *Telematics and Informatics* 129.

2. Organisation for Economic Co-operation and Development (OECD), *Digital Security Risk Management for Economic and Social Prosperity* (OECD Publishing 2015).

3. Douglas W Arner, Janos Barberis and Ross P Buckley, 'The Evolution of Fintech' (2016) 37 *Northwestern Journal of International Law and Business* 127.

4. Verizon, *2025 Data Breach Investigations Report* (Verizon 2025).

5. Reserve Bank of India, *Master Direction on Digital Payment Security Controls* (RBI 2021).

6. Financial Stability Board, *The Financial Stability Implications of Artificial Intelligence* (FSB 2024).

[41] Yinglian Xie, Fang Yu and Martin Abadi, 'De-Anonymizing the Internet Using Unsupervised Machine Learning' (2012) 7 IEEE Security and Privacy 45.
[42] Reserve Bank of India, Master Direction on Digital Payment Security Controls (updated from time to time).
[43] Reserve Bank Integrated Ombudsman Scheme, Reserve Bank of India Integrated Ombudsman Scheme, 2021.
[44] European Banking Authority, 'Report on Machine Learning for Internal Ratings-Based Models' (2021).
[45] Steven Furnell and Nathan Clarke, 'Power to the People? The Evolving Recognition of Human Aspects of Security' (2012) 31 Computers & Security 983.

7. World Bank, *The Global Findex Database 2021* (World Bank 2022).

8. International Telecommunication Union, *Measuring Digital Development: Facts and Figures 2024* (ITU 2024).

9. Basel Committee on Banking Supervision, *Principles for Operational Resilience* (Bank for International Settlements 2021).

10. Europol, *Internet Organised Crime Threat Assessment 2024* (Europol 2024).

11. Lorrie Faith Cranor, *Security and Usability: Designing Secure Systems That People Can Use* (O'Reilly Media 2005).

12. European Banking Authority, *Guidelines on ICT and Security Risk Management* (EBA 2019).

13. World Economic Forum, *Global Cybersecurity Outlook 2025* (WEF 2025).

14. Johnson Kh and others, 'Artificial Intelligence in Banking: Ethical and Regulatory Challenges' (2023) 18 *Journal of Financial Regulation and Compliance* 201.

15. APWG, *Phishing Activity Trends Report* (Anti-Phishing Working Group 2024).

16. National Institute of Standards and Technology, *Digital Identity Guidelines* (NIST SP 800-63B, 2023).

17. National Institute of Standards and Technology, *Cybersecurity Framework 2.0* (NIST 2024).

18. Center for Internet Security, *CIS Critical Security Controls Version 8* (CIS 2021).

19. Alan F Westin, *Privacy and Freedom* (Atheneum 1967).

20. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation).

21. Nora Ni Loideain, *EU Data Privacy Law and Serious Crime* (Oxford University Press 2019).

22. Joseph Bonneau and others, 'The Quest to Replace Passwords' (2012 IEEE Symposium on Security and Privacy).

23. Serge Egelman, Lorrie Faith Cranor and Jason Hong, 'You've Been Warned' (2008) CHI Proceedings 1065.

24. Kern Alexander, 'Banking Supervision in the United Kingdom and the Euro Area' (2023) 44 *Company Lawyer* 98.

25. World Economic Forum, *The Future of AI in Financial Services* (WEF 2024).

26. Maruf Hossain and others, 'The Role of Perceived Security in Mobile Banking Adoption' (2019) 57 *International Journal of Bank Marketing* 215.

27. Basel Committee on Banking Supervision, *Principles for Operational Resilience* (Bank for International Settlements 2021).

28. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) [2016] OJ L119/1.

29. Financial Stability Board, *Cyber Incident Reporting: Existing Approaches and Next Steps for Broader Convergence* (FSB 2023).

30. Organisation for Economic Co-operation and Development, *OECD Framework for the Classification of AI Systems* (OECD Publishing 2022).

31. National Institute of Standards and Technology, *Cybersecurity Framework (CSF) 2.0* (US Department of Commerce 2024).

32. Daniel J Solove, *Understanding Privacy* (Harvard University Press 2008).

33. European Banking Authority, *Report on Machine Learning for Internal Ratings-Based Models* (EBA 2021).

34. Reserve Bank of India, *Master Direction on Digital Payment Security Controls* (RBI, 18 February 2021).

35. M Lynne Markus and Daniel Silverman, 'A Foundation for the Study of IT Effects: A New Look at DeSanctis and Poole's Concepts of Structural Features and Spirit' (2008) 32 Journal of the Association for Information Systems 609.

36. International Organization for Standardization, ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems.

37. Finale Doshi-Velez and Been Kim, 'Towards a Rigorous Science of Interpretable Machine Learning' (2017) arXiv preprint arXiv:1702.08608.

38. Daniel J Solove, 'Privacy Self-Management and the Consent Dilemma' (2013) 126 Harvard Law Review 1880.

39. Karen Renaud and Judith Ramsay, 'Now What Was That Password Again? A More Flexible Way of Identifying and Authenticating Our Seniors' (2007) 23 Behaviour & Information Technology 369.

40. Ann Cavoukian, 'Privacy by Design: The 7 Foundational Principles' (Information and Privacy Commissioner of Ontario, 2011).

41. Yinglian Xie, Fang Yu and Martin Abadi, 'De-Anonymizing the Internet Using Unsupervised Machine Learning' (2012) 7 IEEE Security and Privacy 45.

42. Reserve Bank of India, Master Direction on Digital Payment Security Controls (updated from time to time).

43. Reserve Bank Integrated Ombudsman Scheme, Reserve Bank of India Integrated Ombudsman Scheme, 2021.

44. European Banking Authority, 'Report on Machine Learning for Internal Ratings-Based Models' (2021).

45. Steven Furnell and Nathan Clarke, 'Power to the People? The Evolving Recognition of Human Aspects of Security' (2012) 31 Computers & Security 983.