Life, Work and Connectivity in the Times of SIM-Binding

Perspectives from Consumers and Small Businesses Across India

CUTS International
Since 1983

#2603

Life, Work, and Connectivity in the Times of SIM-Binding

Perspectives from Consumers and Small Businesses Across India

Prepared by

CUTS International
D-217, Bhaskar Marg, Bani Park, Jaipur 302016, India
Tel: +91.141.2282821, Fax: +91.141.2282485
Email: cuts1@cuts.org, Web site: www.cuts-international.org

Author: Krishaank Jugiani, Senior Research Associate, CUTS International. For any clarifications or further details, please feel free to contact him at: kju@cuts.org

Citation: Jugiani, K. (2026). Life, Work, and Connectivity in the Times of SIM-Binding: *Perspectives from Consumers and Small Businesses Across India*. CUTS International.

Acknowledgement: The author is grateful for the support and guidance of Amol Kulkarni, Director (Research), CUTS International (amk@cuts.org)

#2603

Table of Contents

Acknowledgement

I acknowledge the numerous individuals who contributed to the success of this report through their inputs, reviews, and guidance. I extend my sincere gratitude to the survey respondents, including consumers and small and medium businesses, whose valuable insights have been instrumental in shaping this report.

I am particularly grateful to Amol Kulkarni, Director (Research), CUTS International, for his continued guidance, insightful feedback, and unwavering support throughout the research and drafting of this report. I also acknowledge the efforts of Yamini Kumawat (Programme Team), Keval Sharma (Information Technology Team), Madhuri Vasnani and Mukesh Tyagi (Publications Team) at CUTS International for their exceptional support in bringing this report to fruition.

I express gratitude to all individuals, whether named above or not, without whom the publication of this report would not have been possible.

Any remaining errors are solely my responsibility.

Krishaank Jugiani
Senior Research Associate
CUTS International

Executive Summary

In November 2025, the Department of Telecommunications (DoT) issued directions to select Telecommunication Identifier User Entities (TIUEs), including OTT messaging platforms. The Directions respond to rising concerns about cyber fraud, impersonation, and cross-border scams allegedly facilitated by accounts that remain active even after a SIM is removed, replaced, or reassigned.

To address these perceived gaps in authentication and traceability, the Directions mandate two significant measures. First, messaging accounts must remain continuously bound to the same SIM card in the same physical device used at registration. Second, web or desktop sessions must automatically log out every six hours, requiring repeated re-authentication. The stated objective is to strengthen security, improve traceability, and support law enforcement investigations. Platforms are required to comply within 90 days, with enforcement action and reporting within 120 days.

This report evaluates the perceived real-world implications of these measures through consumer and small and medium business (SMB) surveys covering 4,200 respondents —3,600 individual consumers and 600 SMBs — across diverse socio-economic, geographic, and occupational groups. The analysis combined descriptive statistics with multivariate techniques, including binary and ordered logistic regression models, to identify whether there could be any digital inconvenience or operational disruption, and the reasons therefor, arising from SIM-binding and forced logout requirements.

Marginal effects were calculated to translate statistical relationships into intuitive probability changes, enabling policy-relevant interpretation while controlling for confounding demographic and operational variables. The findings indicate that while the security rationale is legitimate, the prescribed implementation risks create widespread friction, exclusion, and unintended economic costs due to a mismatch between regulatory assumptions and actual digital practices in India.

At the household level, device and SIM sharing is widespread. Survey data show that 86 percent of respondents allow family members to use their phone or SIM for messaging. Regression analysis indicates that respondents in shared-device households report lower perceived inconvenience from authentication requirements. However, this finding does not necessarily imply the absence of friction. Instead, it may reflect concentration of authentication control with the primary SIM holder.

Survey data shows that 39 percent of primary SIM holders report being physically away when family members operate their own messaging applications linked to the respondents' SIMs. In such cases, real-time OTP-based authentication may require coordination with the SIM holder, potentially introducing delays for dependent users. In such arrangements, any disruption to the primary SIM — whether due to loss, network issues, reissuance, or travel — can interrupt access for all dependent users. The resulting impact may therefore be collective rather than individual, potentially affecting communication, education, or financial access for multiple household members. This suggests that strict SIM-binding requirements may have uneven effects across users, raising considerations around autonomy, privacy, and digital equity.

Web-based access is similarly central to everyday communication. Nearly 88 percent of respondents use messaging apps on devices without SIM cards, such as laptops, often for sustained periods. Survey responses indicate that inconvenience is associated with proposed requirements such as automatic six-hour session logouts and repeated SIM-linked re-authentication. These measures can interrupt ongoing workflows and require users to regain access through a separate SIM-enabled device.

The reported effects are nationwide and concentrated among working-age users (25-40) and middle- to higher-income respondents, groups that rely heavily on web-based messaging for employment, higher education, and service delivery. For these users, repeated re-logins disrupt active workflows rather than merely causing momentary inconvenience.

Multi-device and multi-SIM usage — reported by over 80 percent and 60 percent of respondents respectively — reflect adaptive practices that support resilience, travel, work-life separation, educational access, and continuity amid device, network, or connectivity constraints. While experienced users may report lower perceived inconvenience, potentially reflecting familiarity with digital authentication processes, regression analysis indicates that OTP-based authentication and requirements to re-verify accounts following SIM changes or session expirations are still associated with measurable workflow disruption.

To assess cumulative authentication burden, the report constructs a Digital Inconvenience Index covering four common scenarios: repeated web re-logins, OTP entry on secondary devices, authentication barriers when the primary SIM is unavailable, and restrictions linked to shared SIM or device usage. Exposure is highly concentrated. Nearly 80 percent reported they might face three or more such frictions, and 49.9 percent reported likely exposure to all four, if the Directions are implemented in their present form.

These effects are particularly pronounced among older users and high-income, digitally intensive users who rely on uninterrupted access across multiple devices. International travel further increases reported inconvenience, as access models that

depend on active primary SIM availability may require users to retain physical access to their registered SIM, obtain roaming connectivity, or rely on alternative authentication steps. Survey responses suggest that such scenarios can complicate access during travel, even if workarounds exist.

For SMBs surveyed across urban, semi-urban, and rural India, OTT messaging platforms are not optional tools but core operational infrastructure. They are used for customer support, order confirmations, vendor coordination, delivery updates, appointment scheduling, and internal team communication. The survey reveals that 73 percent of SMB respondents rely on Wi-Fi-based messaging, 58 percent use web interfaces, 63 percent operate across multiple devices, and 47 percent depend on API or cloud-based integrations to manage customer engagement and workflows. Shared account access is also common, with 65 percent of businesses enabling multiple employees to use the same messaging account for customer support, order management, and coordination. These patterns indicate that messaging services function as embedded business systems rather than standalone communication tools.

Under continuous SIM-binding and six-hour logout requirements, existing business workflows may become more interruption-prone. While the act of re-authentication itself may take only a short time, regression analysis indicates that web-dependent and API-integrated businesses reported 18-21 percentage points increase in anticipated severe operational disruption compared to firms that rely primarily on single-device, SIM-linked usage. This suggests that the impact is concentrated among digitally intensive businesses rather than uniformly distributed across all firms.

The distinction between inconvenience and disruption is important. Entering an OTP may represent minor inconvenience at the individual level. However, for businesses that depend on uninterrupted web dashboards, shared logins, or automated messaging flows, even short authentication breaks can pause customer interactions, delay responses, interrupt automated notifications, or require staff coordination to restore access. Over time, repeated interruptions can accumulate into workflow inefficiencies.

Some businesses may choose to shift toward more formal API-based solutions to reduce session instability or manage authentication centrally. For micro-enterprises operating on thin margins, this could introduce recurring compliance-related costs unrelated to revenue expansion, reaching up to ₹375n per year. Survey responses suggest that this cumulative impact — combining service costs, productivity losses, and coordination overhead — would be felt most acutely by e-commerce sellers, platform-based firms, and internationally active businesses that rely heavily on continuous messaging access.

Importantly, awareness of the regulations does not appear to substantially mitigate anticipated operational impact. Businesses reporting full or partial awareness still

indicated a 58–62 percent likelihood of negative impact from the directive — comparable to firms with limited awareness. Regression analysis further shows that awareness is not a statistically significant mitigating factor once web, multi-device, and API dependencies are controlled for ($p > 0.1$).

These findings suggest that the anticipated impact is linked more closely to workflow structure than to information gaps. Once dependency on web interfaces, shared access, and automated integrations is accounted for, geographic location—including urban concentration — does not significantly alter projected disruption. This indicates that even highly digitised, urban business ecosystems that are deeply integrated with messaging platforms may face similar operational adjustments, underscoring that the effects are tied to usage architecture rather than regional characteristics.

The evidence points to a central conclusion: strengthening digital security is essential, but rigid, technology-prescriptive measures such as continuous SIM-binding and mandatory session expiry may not be well aligned with prevailing patterns of multi-device, shared, web-based, and business-integrated usage across India.

As earlier sections show, messaging platforms support educational continuity, professional coordination, small business operations, and household communication. Measures that introduce repeated authentication or constrain cross-device access may therefore have broader workflow implications, particularly for shared households and digitally intensive enterprises.

The report recommends a calibrated approach. Policymakers should undertake formal regulatory, technical, and privacy impact assessments before implementation. Any studies or independent evaluations publicly claimed should support fraud-reduction benefits. The specific relevance and effectiveness of SIM-binding in addressing identified security threats should also be transparently examined, and alternative mechanisms comparatively evaluated to ensure the most proportionate and effective response. Key technical design variables, such as session expiry duration and re-authentication frequency for web re-logins, should be tested through regulatory sandboxes prior to full rollout. SIM KYC processes should be strengthened at the point of issuance, particularly for bulk or high-volume allocations. Security measures should be risk-based and evidence-driven and developed through structured stakeholder consultation.

A forward-looking digital governance framework can simultaneously reinforce trust, economic participation, and user protection, ensuring that regulatory interventions enhance resilience without disrupting everyday digital practices on which millions depend.

Introduction and Regulatory Context

The advent of digital communication platforms has been one of the most transformative developments in India's telecommunications landscape over the last decade. Driven by rapid smartphone adoption, ubiquitous mobile connectivity, and affordable data services, over-the-top (OTT) messaging applications have become central to how millions of Indians communicate daily.

As of late 2025, India's digital ecosystem continued to expand rapidly, with nearly 1.02 billion internet users, most of whom accessed the internet via smartphones.[1] Messaging platforms dominate online activity, with over 536 million WhatsApp users[2] and 213 million Snapchat users,[3] making India one of the largest markets globally for both. Daily engagement is intense, with users checking apps multiple times and spending hours online, reflecting a strong mobile-first behaviour. This combination of scale, accessibility, and persistent usage has positioned OTT messaging platforms at the heart of everyday communication, social interaction, and increasingly, business engagement across India.

These liberal regulatory approaches were rooted in a broader policy framework governing internet service, in which platforms were not subject to the same stringent licensing, quality-of-service, or interception requirements as traditional telecom carriers. This reflected an underlying philosophy that minimal regulation and reliance on industry-led norms would spur innovation and competition in the digital ecosystem.[4]

In this model, the mobile number served as a digital identifier. Once verified, the messaging application could continue to function independently of the SIM's presence in the device, even if the SIM is removed, replaced, deactivated, or moved across borders. This approach enabled frictionless user experiences across devices and usage scenarios, but also created security and traceability gaps, such as accounts remaining active without a SIM, which regulators note are being exploited for large-scale, often

[1] India's vast internet, social media apps market, Reuters, available at: https://www.reuters.com/business/media-telecom/indias-vast-internet-social-media-apps-market-2026-01-29/

[2] WhatsApp User Statistics: How Many People Use WhatsApp?, Backlinko, available at: https://backlinko.com/whatsapp-users

[3] *Ibid*

[4] No regulation needed for communication apps: TRAI, Times of India, available at: https://timesofindia.indiatimes.com/business/india-business/no-regulation-needed-for-communication-apps-trai/articleshow/78115916.cms

cross-border digital fraud, anonymous scams, and impersonation calls using Indian numbers.[5]

However, in November 2025, the Department of Telecommunications (DoT) issued Directions addressed to specific Telecommunication Identifier User Entities (TIUEs)[6] that provide app-based communication services in India and that rely on mobile numbers either for user identification, authentication, or service delivery.[7] The direction names the TIUEs to which it applies, namely WhatsApp, Telegram, Signal, Arattai, Snapchat, Sharechat, Jiochat, and Josh.

This newly introduced measure introduces two core obligations with far-reaching implications for the design and operation of app-based communication platforms.

First, it requires that such applications remain continuously linked to the same Subscriber Identity Module (SIM)[8] on the same physical device used for registration. This requirement is intended to ensure that account access remains anchored to a verifiable, physically present telecom identifier, thereby preventing continued account use after SIM removal, loss, or reassignment, and strengthening traceability for law enforcement purposes. This continuous linkage replaces the historical verify-once, use-anywhere model and could have far-reaching implications for users, platform operators, and the broader digital ecosystem.

Second, the Directions mandate that all web- or desktop-based sessions of such applications must automatically log out every 6 hours, requiring re-authentication to continue use. This requirement is explicitly designed to limit unauthorised remote access, reduce the window of opportunity for account takeover, and ensure that session continuity remains tied to an authenticated device.

---

[5] Government warns WhatsApp, Telegram and other messaging apps: Within 90 days, make sure your app stops working if…, Times of India, available at: https://timesofindia.indiatimes.com/technology/tech-news/government-warns-whatsapp-telegram-and-other-messaging-apps-within-90-days-make-sure-your-app-stops-working-if/articleshow/125686463.cms

[6] TIUE means a person, other than a licensee or authorised entity (telecom operator), which uses telecommunication identifiers (like mobile numbers) for the identification of its customers or users, or for provisioning, or delivery of services. It was introduced as a new category under the Telecommunications (Telecom Cyber Security) Amendment Rules, 2025 notified under the Telecommunications Act, 2023.

[7] DOT's directions for SIM binding for prevention of misuse of telecommunication identifiers for ensuring telecom cyber security, Department of Telecommunications, (Press Information Bureau release), available at: https://sancharsaathi.gov.in/SancharSaathiDocuments/ImportantDocuments/DOT%E2%80%99s%20directions%20for%20SIM%20binding%20for%20prevention%20of%20misuse%20of%20telecommunication%20identifiers%20for%20ensuring%20telecom%20cyber%20security.pdf

[8] A SIM (Subscriber Identity Module) is a small card or chip that is inserted into a mobile phone. It stores phone numbers and other important information so the phone can connect to the mobile network and make calls, send messages, or use data. Essentially, the SIM acts like an ID card for the phone, identifying the device to the network so the user can use mobile services. GSM 02.17 – Version 3.2.0 – European digital cellular telecommunications system (phase 1); Subscriber Identity Modules, Functional Characteristics, ETSI, available at: https://www.etsi.org/deliver/etsi_gts/02/0217/03.02.00_60/gsmts_0217sv030200p.pdf

DoT has framed these changes as necessary responses to rising cyber threats, particularly those exploiting vulnerabilities in user authentication and number verification. In line with government objectives, the Directions aim to close a critical security gap that allowed accounts to remain active even after a SIM was removed, deactivated, or replaced. This is a loophole that regulators have noted has been exploited in cross-border digital fraud, including phishing, impersonation, account takeovers, and large-scale fraud. The government has reported cyber-fraud losses exceeding ₹22,800 crore in 2024.[9]

By requiring each account to remain continuously linked to a physically present SIM, the government seeks to strengthen traceability, prevent fraud, and support law enforcement and cybersecurity agencies in investigating and mitigating telecom-related cybercrimes.[10]

However, the effectiveness of SIM binding may be limited by weaknesses in KYC processes, which can allow fraudulent or stolen identities to bypass verification. Weak subscriber verification, combined with SIM swaps or compromised credentials, means that simply tying accounts to a physical SIM may not fully close the gaps in authentication and traceability.[11]

Experts also note that SIM-binding may lock an app to a SIM, but not necessarily to a verified real-world identity. As long as fake and mule SIMs circulate and social engineering remains prevalent, fraudsters may continue to bypass the system. SIM binding should therefore be treated as one layer of defence, rather than a complete solution. Without stronger KYC enforcement, robust identity proofing, device controls, and transaction monitoring, fraudsters are likely to pivot to other vectors, such as synthetic identities, mule accounts or hybrid attacks that combine social engineering with device-oriented fraud.[12]

Further, the implementation timetable under the new rules reflects the urgency with which the government seeks compliance. Platforms are given 90 days from notification (dated November 28, 2025) to implement continuous SIM verification and session logout mechanisms, failing which they risk enforcement action under the Telecommunications Act and associated cyber security rules, recently amended in

[9] DoT Mandates SIM-Binding for Messaging Apps to Curb Digital Fraud, DD News On Air, available at: https://www.newsonair.gov.in/dot-mandates-sim-binding-for-messaging-apps-to-curb-digital-fraud/

[10] SIM binding to discourage fraud, strengthen security: Jyotiraditya Scindia, ETTelecom, available at: https://telecom.economictimes.indiatimes.com/news/policy/sim-binding-mandate-to-combat-fraud-and-enhance-national-security-insights-from-jyotiraditya-scindia/127885007

[11] Comments on the Draft Telecommunications (Telecom Cyber Security) Amendment Rules, 2025, CUTS CCIER, available at: https://cuts-ccier.org/pdf/comments-on-the-draft-telecommunications-amendment-rules-2025.pdf

[12] DoT's SIM-binding Mandate Creates New Compliance Challenge, Entrepreneur India, available at: https://india.entrepreneur.com/technology/dots-sim-binding-mandate-creates-new-compliance-challenge/500323

October 2025.[13] Additionally, platforms may be required to submit detailed compliance reports within 120 days, documenting how they have integrated these mandates into their systems.

While the government's intent behind the Directions to combat cybercrime and protect citizens is laudable, the practical implementation of continuous SIM-binding and enforced session expiry presents significant friction for ordinary users and platform operators alike. The mandatory presence of a SIM card in a primary device at all times may disrupt legitimate usage scenarios, such as multi-device workflows (e.g., accessing web clients on laptops or tablets), shared device households, and cross-border travel, where users may legitimately access messaging services via Wi-Fi or secondary devices without the physical SIM present.[14]

These requirements could impose disproportionate burdens, disrupt the user experience, and raise concerns that they extend beyond the Act's statutory remit.

App-based messaging services are deeply integrated into India's social, economic, and professional life, serving not just as consumer applications but as essential communication tools for households, migrant workers, students, journalists, civil society organisations, startups, and small and medium businesses. By specifying authentication methods, device linkage, and session management, the Directions intervene directly in how users access and interact with these services. The Directions focus on specific technological implementations rather than broader security outcomes. Instead of defining objectives such as preventing account takeovers, reducing cross-border fraud, or improving identity verification and encouraging innovations to achieve these objectives, they prescribe continuous SIM linkage and fixed session expiry. This approach raises questions about practicality, proportionality, and compatibility with modern digital practices, where multi-device use, cloud synchronisation, and shared access are common.[15]

Against this backdrop, the Directions warrant close scrutiny–not only for their legality and technical soundness, but also for their real-world impact on everyday users, SMBs, digitally dependent households, privacy, and security outcomes. To understand these concerns, CUTS conducted comprehensive, consumer-focused and SMB-focused surveys across India. The objective of this research was to assess how measures such as continuous SIM-binding and six-hour web logout mandates could affect daily digital experiences, routines, and workflows, and whether the inconvenience and

[13] DoT Notifies Telecom Cybersecurity Rules — What It Means, MediaNama, available at: https://www.medianama.com/2025/10/223-dot-telecom-cybersecurity-rules/

[14] SIM-binding diktat by DoT: Tech firms warn of disruptions for consumers, Business Standard, available at: https://www.business-standard.com/industry/news/sim-binding-diktat-by-dot-tech-firms-warn-of-disruptions-for-consumers-125121601327_1.html

[15] BIF slams SIM-binding directions for msg apps; calls for talks, pause on implementation timelines, The Economic Times, available at: https://economictimes.indiatimes.com/tech/technology/bif-slams-sim-binding-directions-for-msg-apps-calls-for-talks-pause-on-implementation-timelines/articleshow/125721244.cms

disruption, if any, outweigh potential benefits. By capturing the self-reported perspectives of users and SMBs directly impacted by these regulations, the survey provides empirical insights into the operational and behavioural challenges that may arise from implementation.

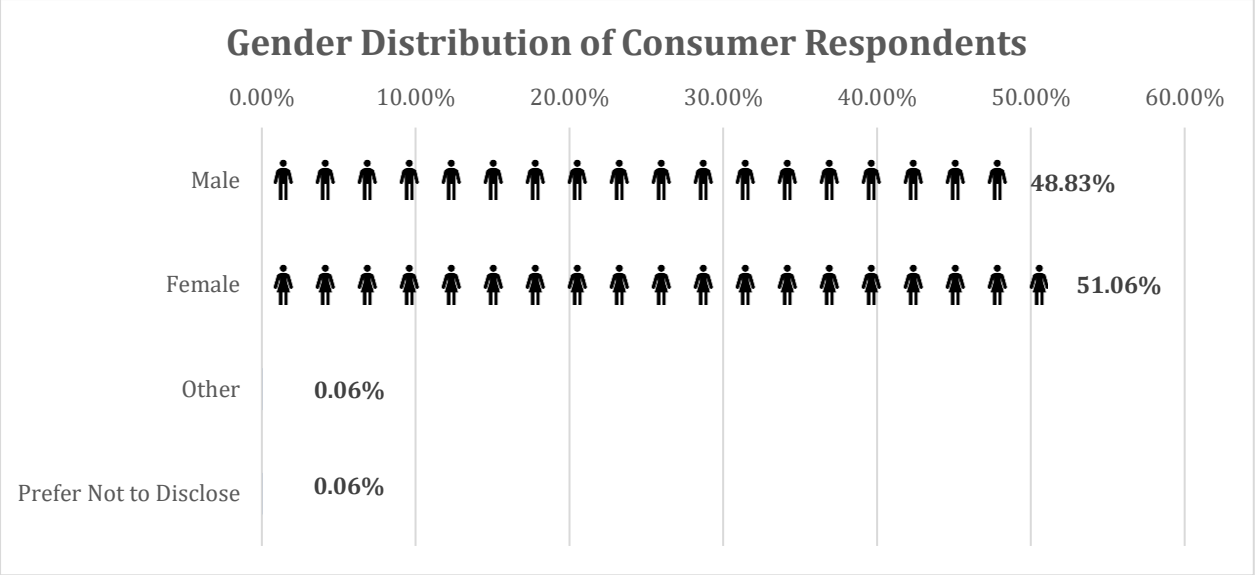
The next sections detail the research methodology, the anticipated impact of the directive on consumers and SMBs, the analysis of survey results, and recommendations. This report thus provides a consumer-centric lens on regulatory changes that, while technical in design, could reshape the way millions of Indians interact with digital communication platforms every day.

Methodology

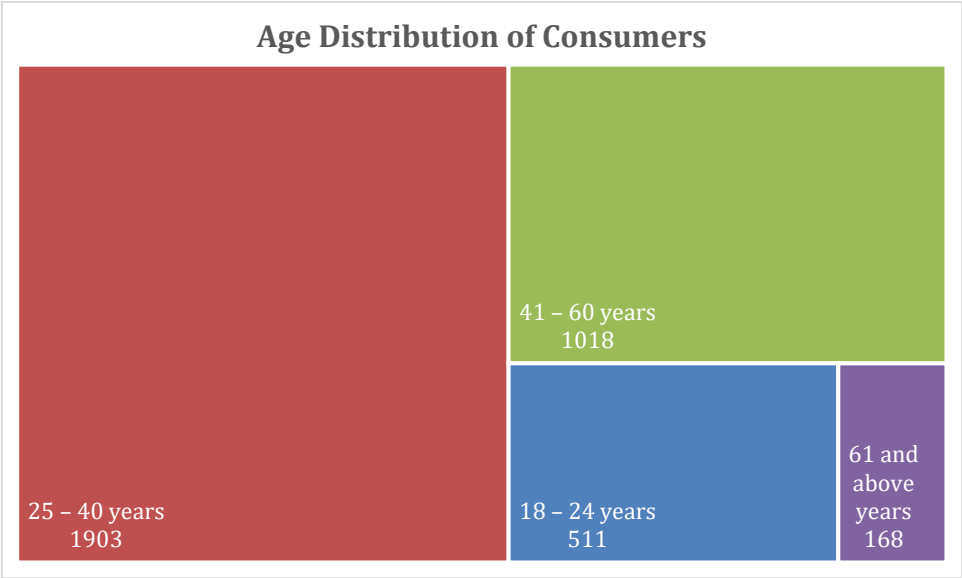
The surveys engaged a diverse set of 4,200 respondents, including 3,600 individual consumers and 600 SMBs, covering multi-device households and professionals. This approach captured variations in device-sharing, SIM usage, and multi-device workflows across geographic, socio-economic, and occupational groups, reflecting the wide-ranging impact of the new directives on digital life in India. Consumer respondents included individuals from low-income households, students, homemakers, seniors, gig workers, and frequent travellers, while SMB respondents included small merchants, entrepreneurs, freelancers, and startups. Respondents were purposively stratified to ensure representation across key demographic and occupational groups.

Survey Locations

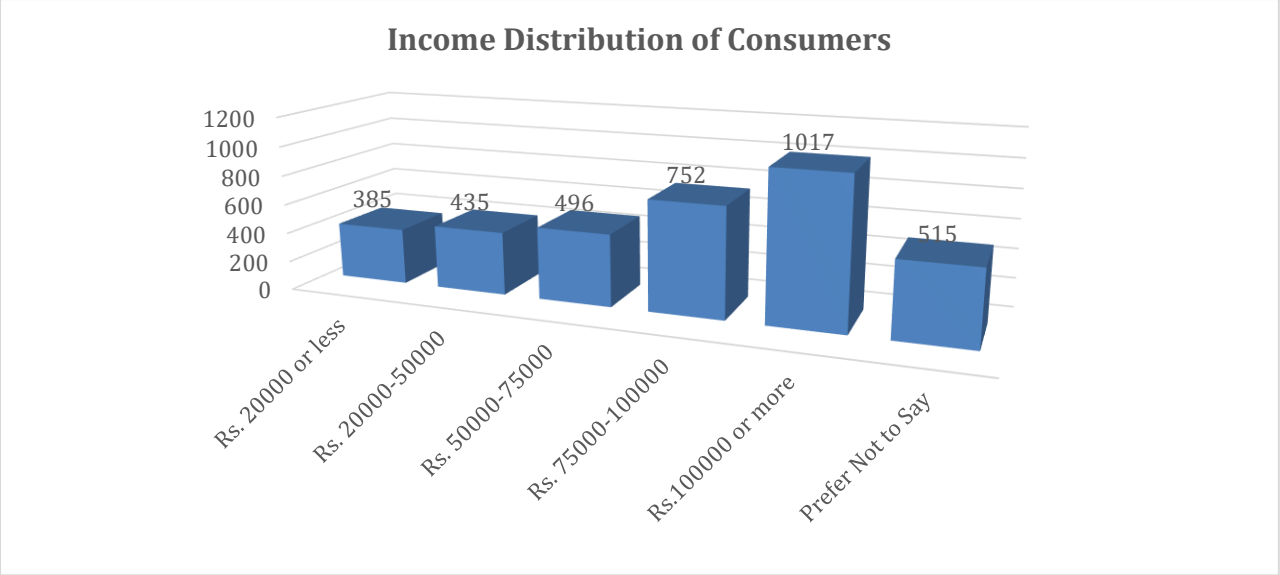
As the survey relied on non-probability sampling, the results aim to provide robust, nationwide, indicative insights into digital practices and user experiences across India, focusing on how individuals anticipate they may behave or be impacted after the implementation of the Directions.



Respondents were asked about their experiences with account access, device usage, cross-device workflows, shared-device arrangements, and cross-border mobility, as well as their perceptions of security, convenience, and usability under the new Directions.

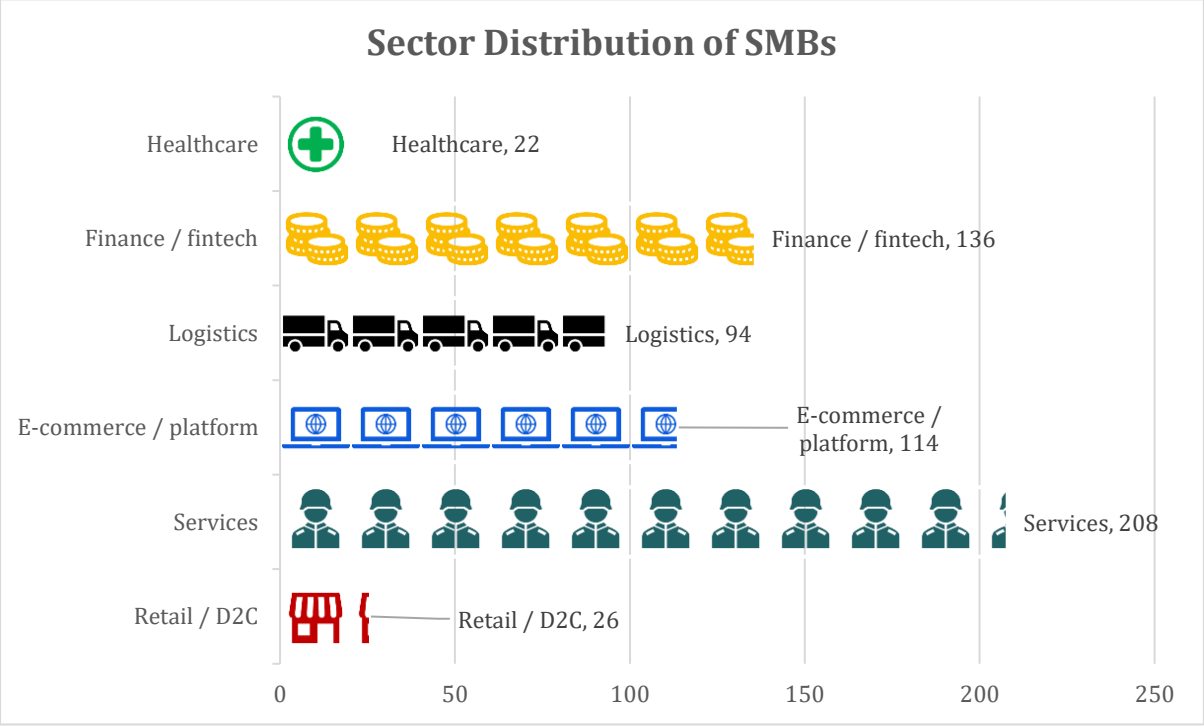


Questions were framed to elicit respondents' anticipated behaviour and perceived impact based on their current digital practices, rather than observed outcomes. They examined multiple dimensions of user experience, including the types of devices used to access communication apps, the frequency of accessing apps on devices without a SIM (such as laptops, tablets, shared household devices, or employer-issued devices), multi-device workflows including companion or web logins, and instances when the SIM was unavailable.

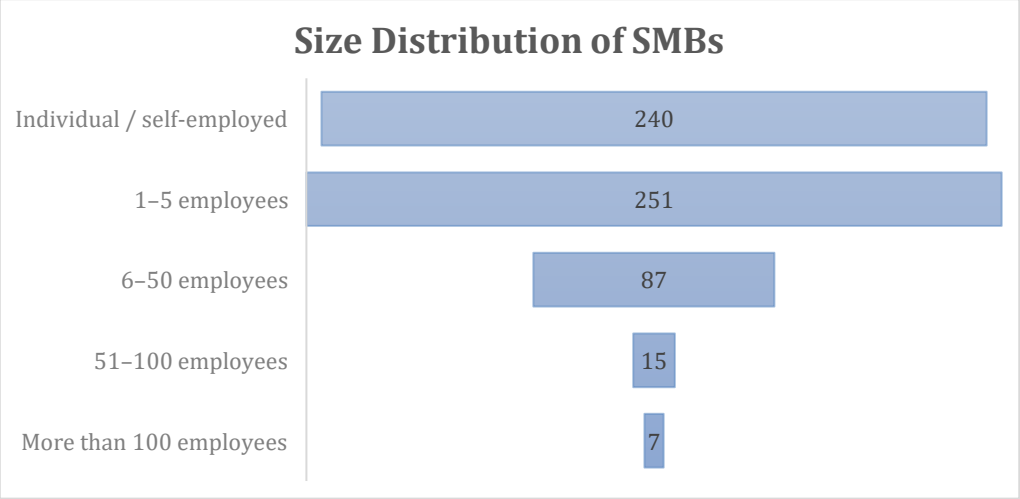


Respondents were also asked for their views on potential disruptions, costs, or exclusions introduced by SIM-binding and forced logout rules.

For SMBs, additional questions focused on shared-number workflows, staff access across devices, dependence on desktop or office-based interfaces, and the operational impact of enforced periodic logouts on transactions, communications, and customer support.



Importantly, the questionnaire included neutral and counterfactual response options, including reporting no disruption or inconvenience. This ensured that the survey did not presuppose negative outcomes and allowed respondents to reflect their actual or expected experiences.



The data from both consumers and SMB surveys were systematically coded, cleaned, and analysed using STATA.

Data Cleaning and Handling of Missing Values: Both surveys were designed with conditional logic, meaning respondents were only asked questions relevant to their experiences. For example, follow-up questions on multi-device workflows were only asked of consumers who reported using multiple devices. No imputation was applied, preserving the integrity of the dataset. Core demographic and unconditional questions had minimal missing data.

Coding and Multiple-Response Questions: In both surveys, responses were pre-coded during questionnaire design to maintain consistency. Multiple-response questions — such as reasons for using Wi-Fi, web-based messaging, shared accounts, or multi-device workflows — were converted from text responses into binary indicator variables.

Descriptive Analysis: Descriptive statistics were used to understand baseline patterns of digital behaviour. For consumers, this included Wi-Fi-based and web-based messaging, multi-device and multi-SIM usage, and shared-device arrangements. Time-use variables helped capture the intensity of reliance on these practices in daily life. For SMBs, analysis focused on business operations, including shared-number workflows, staff access across devices, and anticipated disruptions, if any, from SIM-binding or forced logout rules.

Subgroup analyses were conducted to highlight differences across consumer demographic and geographic groups (e.g., age, gender, income, and region) and across SMB business size, sector, and state. These cross-tabulations revealed which groups are most likely to experience operational friction under new regulations, providing a granular view of distributional impacts.

Regression and Multivariate Analysis:[16] To understand which factors drive potential disruption, regression models were applied in both surveys.

- Binary logistic regression estimated the likelihood of experiencing any operational inconvenience (for consumers) or expecting a negative business impact (for SMBs).
- Ordered logistic regression captured the severity or cumulative number of disruptions, whether in consumer workflows or business operations.

The analysis does not establish causality; rather, it aims to provide stronger evidence on which scenarios are systematically associated with a higher risk of disruption. By controlling for age, income, geography, business size, and other relevant factors simultaneously, the models help separate meaningful patterns from simple correlations. This allows for a clearer understanding of which specific digital practices are likely to be disrupted, rather than merely observing that two factors co-occur. Regression coefficients represent log-odds, which can be exponentiated to produce odds ratios–a more intuitive measure indicating how much more (or less) likely a respondent, business or consumer usage workflow is to experience disruption.

Interpreting coefficients:

- A positive coefficient means the factor increases the likelihood of inconvenience or negative impact. For example, businesses using API-based messaging are more likely to anticipate operational difficulties under SIM-binding requirements.
- A negative coefficient means the factor reduces the likelihood of inconvenience or disruption.
- Marginal effects were calculated to translate statistical coefficients into percentage-point changes in probability, making results easier to interpret for policy audiences.

Model diagnostics and reliability:

- Pseudo R^2 values indicate how well the models explain variation in outcomes, although they are not directly comparable to traditional R^2 in linear regression. Values between 0.2 and 0.3 are typical and acceptable for social science survey data.
- Standard errors and confidence intervals were used to assess statistical precision. Results based on very small subgroups or where standard errors were unusually large were treated cautiously.

[16] Binary logistic regression is a method used to estimate the likelihood that a particular outcome happens. For example, whether a consumer would face any inconvenience or a business anticipates a negative impact.
Ordered logistic regression looks at outcomes that can occur at multiple ordered levels, helping to understand not just whether disruptions happen, but how severe or frequent they are. For example, it was used to capture the cumulative or graded nature of disruptions across workflows or operations, providing insight into variations in intensity or frequency.

- Certain categories (e.g., very small business types or demographic segments) were sometimes omitted from models due to perfect prediction or collinearity, but this did not affect the overall conclusions.

In simple terms, the analysis first examined patterns of digital behaviour among consumers and businesses and then assessed which behaviours or characteristics make them more likely to experience problems under the new regulations. The use of regression models allows for isolating the effect of each factor while controlling for others, ensuring that conclusions about potential disruptions are robust. Where regression results and descriptive patterns align, confidence in the findings is higher.

Certain limitations should be noted. The findings presented in this report are based on self-reported responses, which may be subject to respondent bias, particularly in areas involving sensitive digital practices, such as multi-device use and SIM sharing. Further, some questions were scenario-based or hypothetical, requiring respondents to assess how they expect their behaviour or operations would change under the proposed regulations. As such, responses reflect perceived and anticipated impacts.

Despite this, the regression and descriptive analyses provide a robust empirical basis for understanding how continuous SIM-binding and periodic re-authentication requirements could affect digital access and operational workflows among consumers and small businesses in India. Future studies covering a broader geographic and demographic scope may help validate and refine the trends observed in this research.

Implications for Everyday Users and Households

Sharing of Devices in a Family by the Dependent Users

India's digital landscape is characterised by widespread connectivity, intense device usage, and complex household-level practices. Rural regions account for 57 percent of India's 958 million active internet users, with approximately 548 million users.[17] This demographic reality underscores the importance of accounting for regional and socio-economic diversity in assessing regulatory mandates. Approximately 18 percent of active internet users — around 172 million people — access the internet through shared devices, primarily in rural areas where 80 percent of these shared-device users reside (approximately 138 million).[18]

In these households, a single smartphone often serves as the primary gateway for education, social communication, financial transactions, and other essential digital services. Women, children, and elderly people frequently rely on these devices to access messaging applications, online learning platforms, and government services. For many households, a single smartphone or device serves as the primary gateway to education, financial services, social communication, and essential government platforms. Women, children, and elderly members frequently rely on these shared devices, with women representing 58 percent of shared-device users.[19]

The survey asked where the primary SIM holder is typically located when family members use messaging apps linked to their SIM. 39 percent reported being far away. This indicates that in a significant share of shared-use situations, dependent users may not have immediate access to the primary SIM holder, potentially delaying OTP submission and authentication completion.

Survey data strongly corroborate the prevalence of household-level sharing. The survey explored shared access within households, asking whether family members use the respondent's phone or SIM to operate their own messaging apps. Respondents who answered 'Yes' were asked why, with options including inability to procure SIMs, shared devices, shared SIMs, and safety or monitoring concerns. Overall, 86 percent

[17] India's internet user base crosses 950 million in 2025: IAMAI report, Business Standard, available at: https://www.business-standard.com/industry/news/indian-internet-user-base-crosses-950-million-in-2025-iamai-report-126012901048_1.html
[18] Ibid
[19] Ibid

of respondents reported that family members use their phone or SIM to operate messaging apps, confirming that shared access is not marginal but frequent.

Importantly, the survey instrument positions the respondent as the primary SIM or device holder, while family members are treated as dependent users operating through shared credentials, for various reasons, such as inability to procure separate SIMs, use of separate accounts on a single SIM, sharing of one phone, and for safety or monitoring purposes.

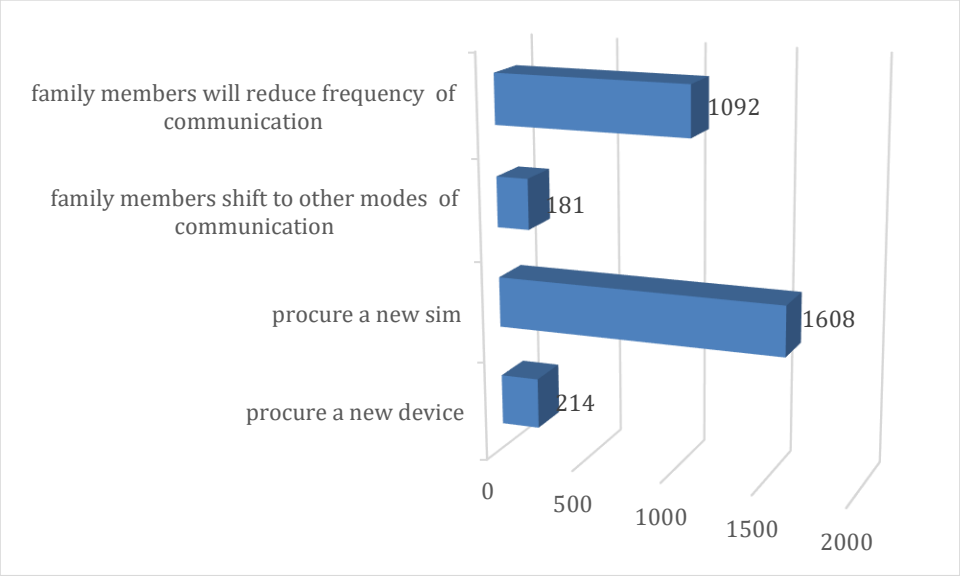
The regression analysis shows that respondents who report sharing their phone or SIM card with family members, on average, report lower overall authentication or OTP-related inconvenience. In the cumulative model that combines different types of authentication friction, family sharing is associated with significantly lower reported inconvenience (coefficient = −1.14, $p < 0.001$). At first glance, this may suggest that households with shared devices or SIMs face fewer authentication problems.

However, this interpretation requires careful explanation. Survey responses show that 39 percent of primary SIM holders report being far away when family members operate messaging apps linked to their SIMs. Since authentication control is centralised with the primary holder — who receives OTPs, completes SIM verification, and manages session relinking — physical absence can create coordination delays. In such cases, dependent users may be unable to complete time-sensitive authentication steps independently, especially where real-time OTP entry is required.

Regression analysis also indicates that lower-income respondents are significantly more likely to report device or SIM sharing. Survey results further show that more than 25 percent of respondents who reported sharing a device or SIM belong to households with monthly incomes below ₹50,000 (excluding those who did not disclose income, n = 3,186). This represents the largest share among all income categories, indicating that shared access practices are particularly prevalent among lower- and lower-middle-income households. These findings suggest that authentication designs requiring individual SIM control may disproportionately affect economically vulnerable households, where shared access is both common and structurally necessary.

Therefore, lower reported inconvenience in shared households does not necessarily mean that authentication friction is absent. Instead, it suggests that the burden is concentrated on one person and measured only through that individual's responses. If a dependent family member has to wait for the primary holder to submit an OTP or is unable to complete a task independently, the coordination cost would need to be recorded separately. The findings thus indicate redistribution of authentication responsibility within households, rather than elimination of authentication-related constraints.

A key follow-up question asked how respondents would react if family members were not permitted to use messaging apps without their own SIMs, capturing potential exclusion effects, such as reduced communication or the need to procure new devices or SIMs. The responses indicate that restrictions on SIM-linked messaging access would not be neutral for shared households. The dominant reaction among the respondents was the need to procure a new SIM, which could place a financial burden on lower-income individuals families, due to the need for repeated recharges.



If family members were not permitted to operate messaging apps without having their own SIMs (n=3095 responses for 3095 respondents)

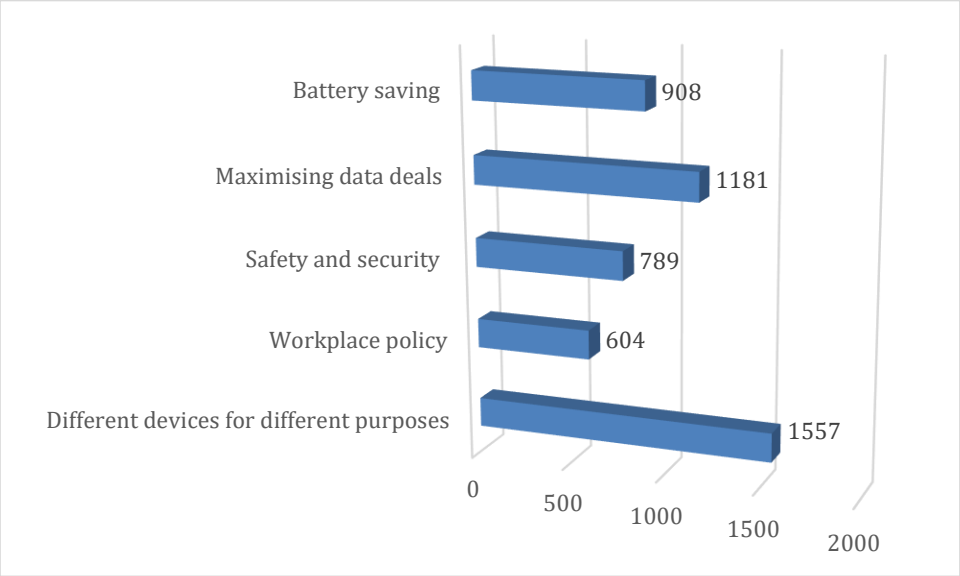
However, a substantial proportion also reported that family members would reduce the frequency of communication, pointing to likely behavioural contraction rather than seamless substitution. This pattern suggests that mandatory individual SIM linkage could generate both financial and participation costs. While some households may absorb the cost of additional SIMs or devices, others may scale back their digital engagement. In lower-income and shared-device households, where access is already centralised and resource-constrained, such requirements may therefore translate into reduced connectivity for dependent users rather than simple formalisation of access.

Cumulatively, these findings suggest that SIM-linked authentication requirements may unintentionally reinforce dependence structures. As highlighted, the apparent statistical reduction in inconvenience among sharing households reflects the concentration of control. If regulatory frameworks require each user to authenticate independently with a personal SIM, households that currently rely on shared access may face higher device acquisition costs, SIM procurement barriers, and potential digital exclusion for women, children, and elderly members.

Use of Same Messaging Apps on Multiple Devices

Multi-device use is widespread in India. A notable 20 percent of active internet users (approximately 193 million individuals) engage in multi-device workflows, with urban users significantly dependent on multiple devices (31 percent in urban areas versus 12 percent in rural regions).[20] These users often use multiple devices—including laptops, tablets, and desktops.

In the survey as well, 81.5 percent of respondents reported using the same messaging apps on more than one device, such as a smartphone and laptop, a phone and tablet, or multiple phones. Commonly reported reasons include separating work and personal use, managing battery life and device limitations, complying with workplace policies requiring desktop access, addressing security concerns, and navigating shared household arrangements. These responses indicate that multi-device use of the same account is generally intentional and structured, reflecting deliberate routines designed to manage time and ease of use.



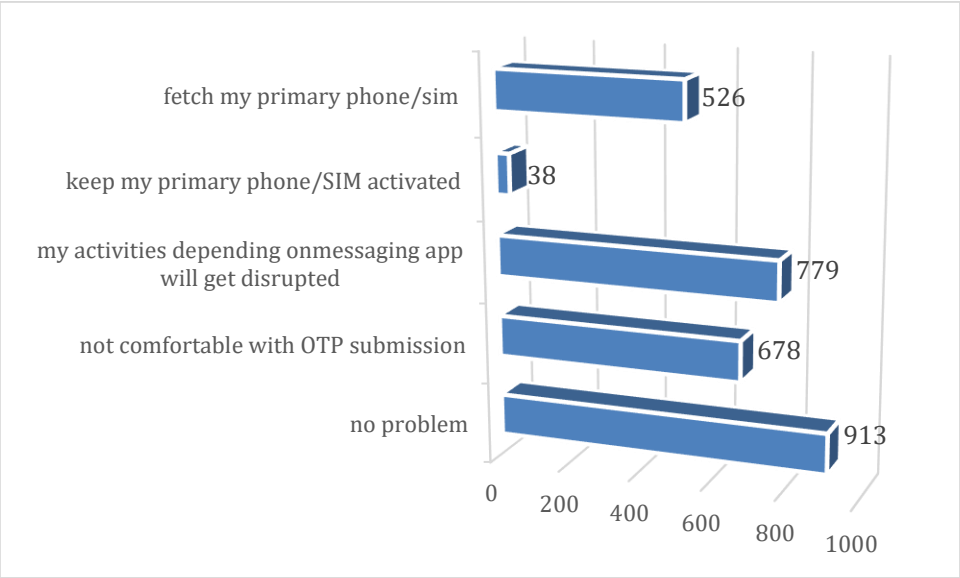
Reasons for using same messaging service on different devices (n=5039 responses for 2934 respondents)

In the ordered logistic regression, multi-device use shows a large, statistically significant positive association (coefficient ≈ +1.63, $p < 0.001$). In simple terms, respondents who already manage messaging apps across multiple devices are substantially more likely to anticipate inconvenience if authentication requirements become stricter. This effect remains robust across model specifications and after controlling for age, gender, income, geographic zone, and international travel. Such users may need to prepare in advance by keeping SIMs active, ensuring devices are nearby, or maintaining persistent sessions — imposing preparation and compliance costs that arise specifically because of authentication requirements.

[20] Ibid

The survey analysis explicitly examined how One-Time Password (OTP)–based authentication may affect users when they access messaging applications on devices other than their primary phone. Respondents were asked whether they experience inconvenience when an OTP is required to log in on a secondary device, such as a laptop, tablet, or desktop. The response options captured escalating levels of disruption, ranging from no inconvenience to minor inconvenience to significant inconvenience that disrupts ongoing work or communication. A related question asked whether switching SIMs or using messaging apps across multiple SIMs would trigger OTP-related disruption, including delays, repeated verification attempts, or inability to continue an ongoing session.

The main challenges reported were disruption of ongoing activities dependent on messaging apps (27 percent), discomfort or difficulty with OTP submission (23 percent), and the need to fetch the primary phone or SIM to complete authentication (18 percent). These responses indicate that SIM-switching or multi-SIM use is not merely a technical adjustment, but can interrupt workflows, delay communication, and create dependence on access to a specific device.



Respondents on needing to periodically submit OTP to continue operating messaging app on a different device/ sim (n=2934 responses for 2934 respondents)

Regression results further show that OTP requirements could be among the most disruptive elements of the authentication process, particularly for users who rely on secondary devices for sustained or work-related use. Binary logit models of OTP inconvenience indicate that when frequent OTPs are required for SIM switching, respondents report substantial workflow disruption and time costs. Multi-device users of the same messaging accounts are therefore particularly prone to encountering OTP requests on secondary devices, forced logouts when switching devices, and repeated

re-verification after inactivity. Such situations may result in inconvenience, with respondents reporting that ongoing tasks would be disrupted, that they would need to fetch or activate the primary phone, or that time-sensitive communication would be delayed, indicating clear time and coordination costs.

In the binary logit model examining OTP inconvenience on secondary devices, age effects are large and statistically strong. Compared to respondents aged 18–24, those aged 25–40 have significantly higher odds of reporting OTP-related inconvenience (coefficient = +2.10, $p < 0.001$). The effect is slightly larger for respondents aged 41–60 (coefficient = +2.19, $p < 0.001$).

Box 1: When Authentication can Interrupt Productive Use

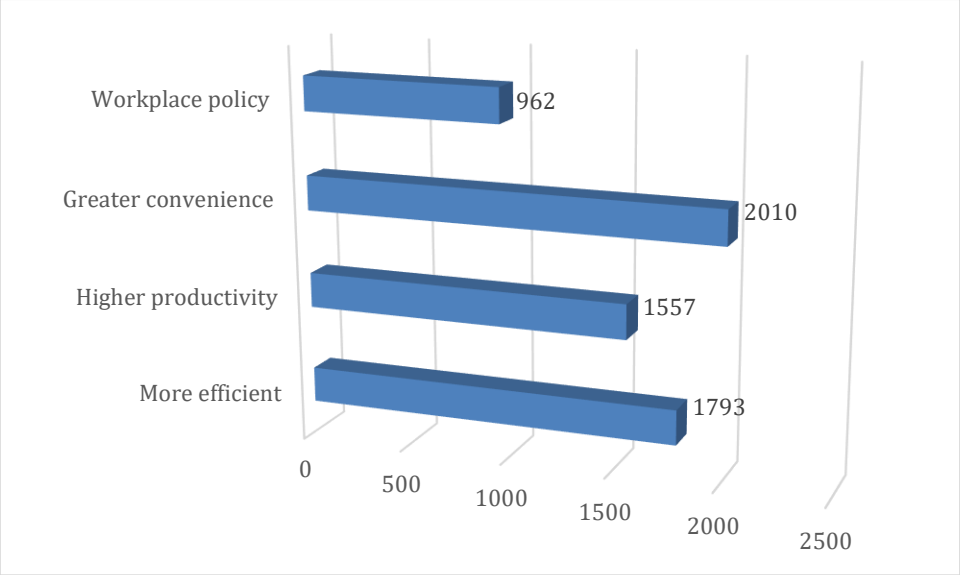
The above findings indicate that older users are far more likely than younger users to report that OTP requirements interrupt their ability to continue using messaging apps on secondary devices. This finding helps clarify earlier ambiguities around age. While younger users may report higher overall sensitivity to inconvenience, working-age and older users would experience the sharpest disruption in specific authentication moments, particularly when OTPs are required mid-task.

For many respondents in the 25-60 age range, secondary devices are not optional conveniences, they are essential tools for work, education, or coordination with family. Being forced to retrieve an OTP from a phone — especially if the phone is elsewhere, switched off, shared, or out of reach — can interrupt meetings, delay responses, or require restarting tasks entirely.

Income effects further reinforce this story. Respondents in higher income brackets show some of the largest coefficients in the model, with OTP inconvenience effects reaching +3.93 ($p < 0.001$). This reflects that these users would be more heavily exposed to OTP-triggering situations because they spend longer hours on laptops and desktops, juggle multiple devices, and rely on continuous access for professional tasks. For these users, each OTP interruption could carry a measurable opportunity cost in time, productivity, and attention.

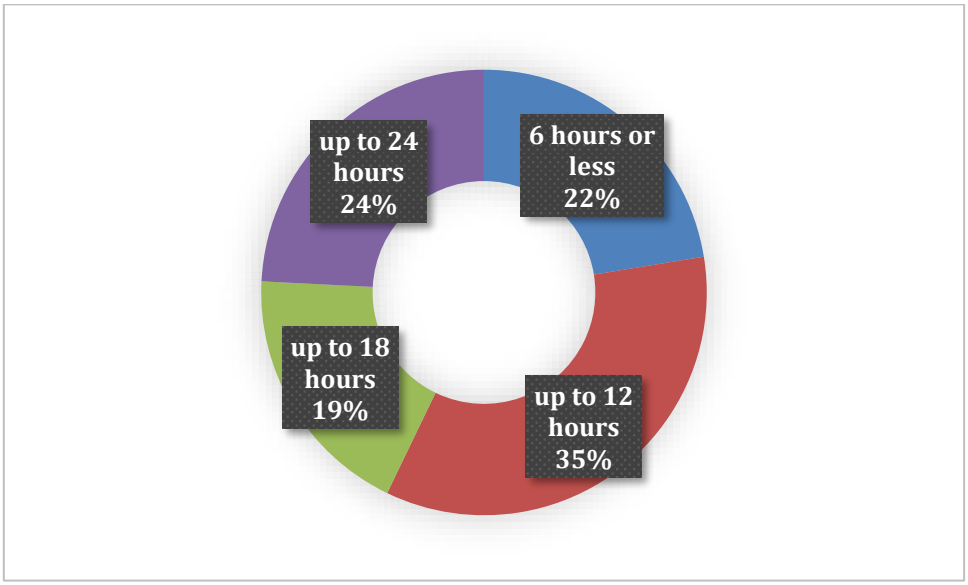
Use of Web Versions of Messaging Apps

The survey explored the use of web-based messaging platforms on laptops or desktops. 88 percent of respondents reported accessing messaging apps on devices with web versions, including laptops, desktops, and tablets.



Reasons for using web versions of messaging apps (n=6322 responses for 3165 respondents)

These findings indicate that web use is deliberate and often linked to productive, time-intensive activities such as office work, education, and coordination tasks that require extended, uninterrupted sessions. Supporting this, time-use data show that among web-based messaging users, more than 75 percent spend more than 6 hours per day logged in. In other words, more than 75 percent respondents spend more than 6 hours on web-based messaging platforms. This persistent presence reflects the expectation that messaging services remain readily accessible on non-SIM devices, particularly in workplace or home-office contexts. Under a six-hour re-login requirement, these users would need to re-authenticate two to three times per day, implying repeated workflow interruptions and generating non-trivial opportunity costs.



Time spent on web versions of messaging apps (n=3165 responses for 3165 respondents)

Importantly, respondents reported inconvenience from frequent web re-logins, including forced re-logins or authentication requirements. In the binary logit model of web re-login inconvenience, respondents aged 25-40 are significantly more likely to report that forced re-logins would be inconvenient (coefficient ≈ +0.45, $p < 0.001$).

Box 2: Repeated Relogins and Disruption of Daily Workflows

This age group of 25–40 corresponds closely to users in full-time employment or higher education, for whom messaging platforms are deeply embedded in daily workflows. Repeated re-logins would interrupt ongoing tasks, delay responses, and require restarting work sessions.

Income effects are also strong. Middle- and higher-income respondents show large, positive, and statistically significant coefficients (Coefficient ≈ +2.0, with $p < 0.001$). This reflects greater exposure, and since these users rely more heavily on web-based messaging for work, coordination, and service delivery, they would face inconvenience due to repeated re-logins.

These findings indicate that inconvenience would arise when authentication systems repeatedly require re-linking to a primary SIM that may be inactive, unavailable, or located elsewhere, since the SIM-based or primary account is used to re-login in web versions.

Use of Wi-Fi on Mobile Phones for Messaging Apps

The survey also examined the use of Wi-Fi on mobile phones for accessing messaging applications. 96 percent of the respondents said they use Wi-Fi for messaging. Most users cited speed, cost savings, and convenience as key reasons. Regression results show a clear pattern in who relies most heavily on Wi-Fi for messaging. Higher-income respondents are significantly more likely to report intensive Wi-Fi-based use. Across higher income brackets, the analysis is statistically significant ($p < 0.001$), indicating that Wi-Fi reliance is not randomly distributed but follows a structured economic gradient.

In simple terms, as income increases, so does the likelihood of sustained Wi-Fi-based messaging. Age patterns are more mixed. However, working-age groups are generally more likely to report extended Wi-Fi use compared to the reference category, suggesting that Wi-Fi is closely linked to professional, educational, and high-frequency communication needs.

At the same time, the regression results show that this intensive, Wi-Fi-enabled environment is associated with greater authentication friction. In the ordered logistic model of cumulative inconvenience, web messaging use has a large positive coefficient (≈ 2.99, $p < 0.001$), and multi-device use also shows a strong positive association (≈

1.63, $p < 0.001$). These magnitudes indicate substantially higher odds of reporting multiple authentication-related disruptions among users operating in web-based and multi-device ecosystems.

Importantly, this means that even highly connected, digitally intensive users—those relying on laptops, desktops, and continuous Wi-Fi access—are likely to experience repeated log-outs, OTP prompts, and session interruptions as meaningful workflow disruptions. At the same time, this does not discount the challenges faced by less digitally active users. For them, authentication barriers may not occur frequently, but when they do, they can require significant effort to reconnect, retrieve credentials, or regain access.

The evidence therefore points to layered disruption across the digital spectrum—frequent workflow interruption at the intensive-use end, and higher re-entry barriers at the lower-use end. Rather than being an isolated inconvenience, authentication friction could be embedded within high-intensity, Wi-Fi-supported communication environments.

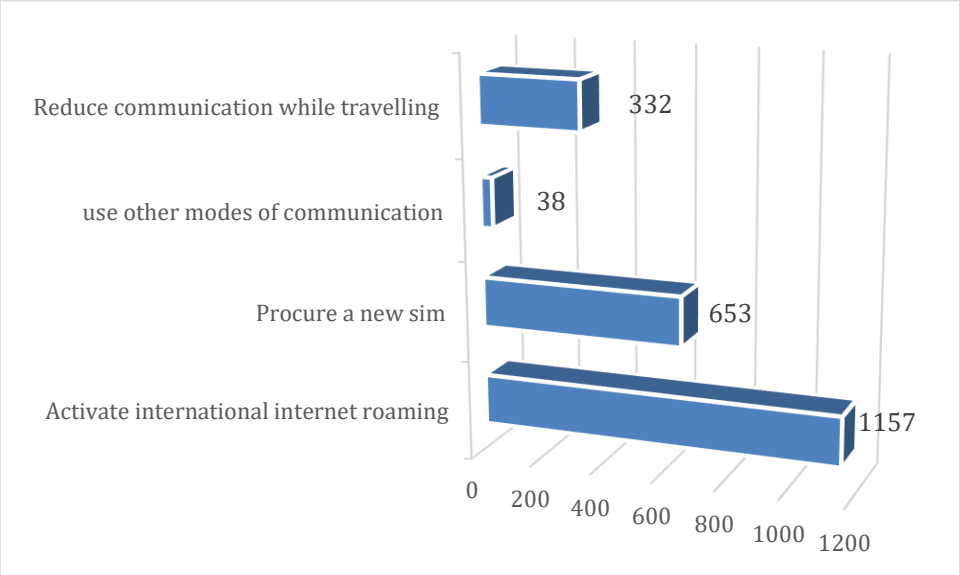
International Travel and Messaging App Use

The survey examined international travel as a distinct usage context, asking respondents whether they frequently travel outside India and use Wi-Fi or local SIM cards abroad for messaging. 60.5 percent of respondents reported travelling outside India and using Wi-Fi or local SIMs to access messaging apps. The most cited reasons include lower cost, lack of support for Indian SIMs abroad, and easy availability of local connections. The survey also examined whether international travel could amplify authentication-related inconvenience, particularly for users who access messaging services while abroad. International travel consistently shows a negative and statistically significant association with reported inconvenience in the aggregate index (coefficient = −0.99, $p < 0.001$).

At first glance, this suggests that international travellers experience less inconvenience. However, this result reflects selection rather than ease. Survey responses indicate that individuals who travel internationally are more likely to report adopting specific access strategies—such as maintaining roaming connectivity, keeping primary SIMs active, or arranging alternative authentication methods in advance. The lower reported inconvenience may therefore reflect preparatory behaviour rather than the absence of friction.

At the same time, disaggregated models reveal that when inconvenience does occur during travel, it is acute. In SIM-related OTP models, international travel is associated with significantly lower odds of inconvenience (coefficient = −1.21, $p < 0.001$), again reflecting preparation and self-selection. This does not mean authentication is frictionless during travel, but rather that users are expected to invest in mechanisms to overcome such frictions. Survey responses to coping strategies suggest that

maintaining access while travelling may require additional planning or expenditure, indicating that cross-border usage can introduce logistical considerations not present in domestic contexts.



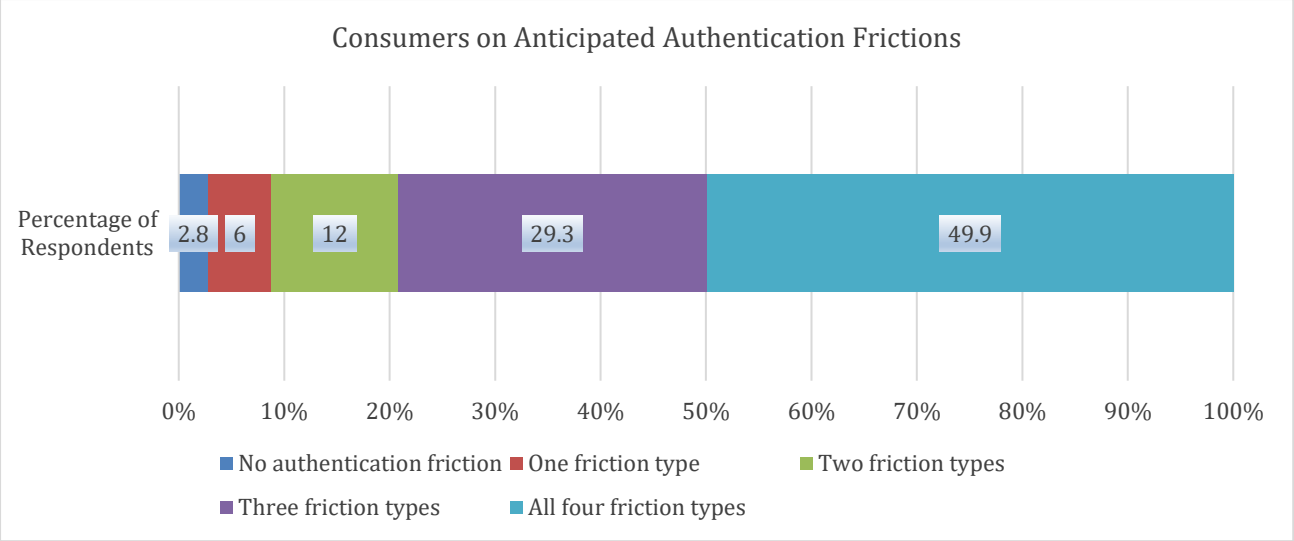
Respondents on how they would react if they were not permitted to use wifi or a local sim for operating messaging apps (n=2180 responses for 2180 respondents)

Cumulative anticipated Inconvenience for consumers

To capture the cumulative nature of authentication-related disruption, the analysis constructs a digital inconvenience index. The index counts the number of distinct authentication-related situations that a respondent reports they would face, based on four survey questions covering common access scenarios:

1. Being required to repeatedly re-login on web-based or desktop versions of messaging applications
2. Being required to enter OTPs when accessing messaging applications on secondary devices
3. Facing authentication problems when the primary SIM is unavailable, inactive, or located elsewhere
4. Facing restrictions due to reliance on shared or family SIMs and devices+

The distribution of this index shows a strong concentration of inconvenience. Only 2.8 percent of respondents reported no exposure to any of the four friction scenarios. Fewer than 9 percent report exposure to at most one. In contrast, nearly 80 percent report exposure to three or more distinct authentication-related frictions, and almost 50 percent report exposure to all four. The mean inconvenience score was 3.19 (with standard deviation = 1.03) on a four-point scale. This indicates that, for most users, authentication-related inconvenience is not limited to a single, occasional disruption, but instead arises through multiple overlapping mechanisms.



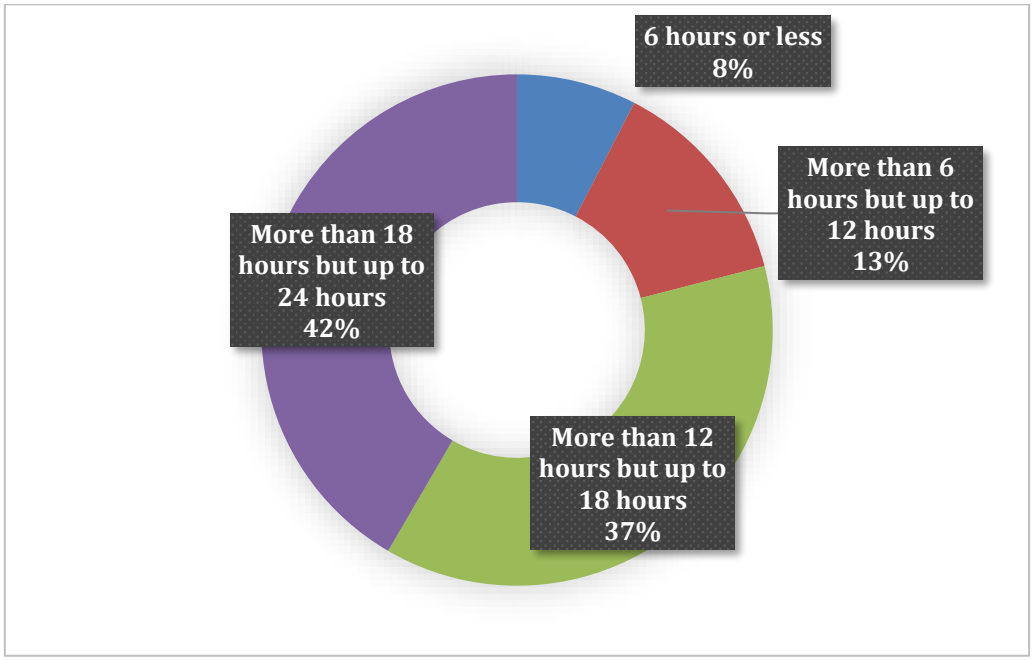
Importantly, the index captures exposure to types of disruption, not the frequency with which they occur. In practice, these frictions manifest as interrupted work sessions, forced task restarts, delays in sending or receiving messages, and dependence on the availability of a specific SIM or household member. For users who rely heavily on web-based or multi-device access, especially for long daily sessions, these disruptions can occur multiple times in a day, compounding time loss and reducing usability. The distribution of the index is right-skewed, reinforcing the idea that authentication-related inconvenience is typically experienced as a cumulative and persistent constraint on everyday digital use, rather than an isolated or occasional disruption.

Impact on Small and Medium Businesses

Across India's SMB ecosystem, ranging from individual entrepreneurs to medium-sized enterprises, OTT messaging platforms function as core business infrastructure rather than auxiliary communication tools, and have become an essential part of business operations. For many SMBs, messaging apps are the primary channel for customer acquisition, order confirmation, after-sales support, supplier coordination, and internal staff communication. To assess vulnerability to SIM-binding and related mandates, the survey asked businesses to anticipate whether such requirements would have no impact, some impact, or a significant negative impact on their operations.

Use of Wi-Fi on Mobile Phones for Messaging Apps

Businesses were first asked about the use of messaging apps on mobile phones through Wi-Fi. Respondents could indicate whether each mode was used rarely, occasionally, or regularly and as an essential part of operations. A vast majority, 92, of SMBs reported that they rely on Wi-Fi for messaging. A major section out of these, again 92 percent said that they use these apps on Wi-Fi for more than 6 hours or more, reflecting the centrality of internet-based access beyond SIM-enabled connectivity.

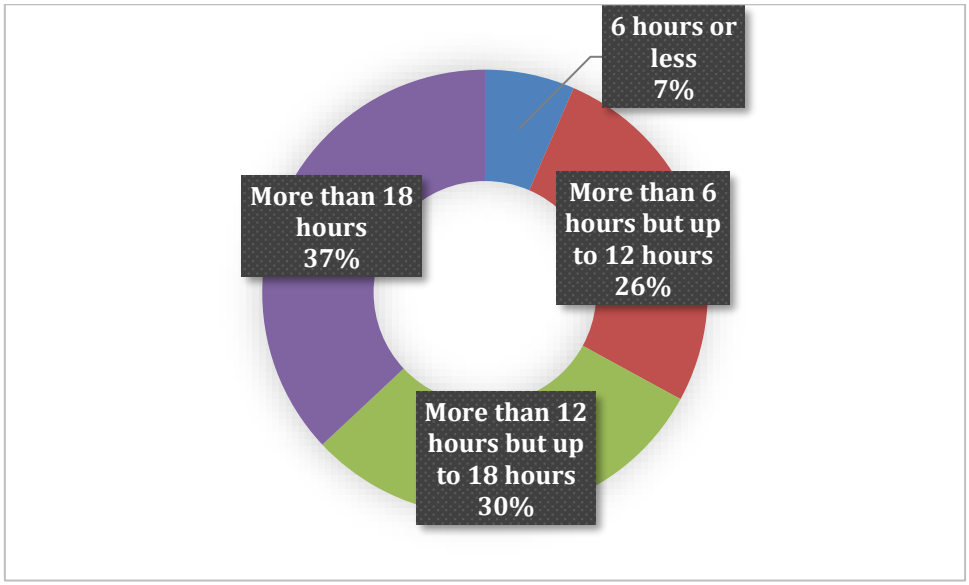


Time for using messaging apps over Wi-Fi (n=553 responses for 553 respondents)

To assess whether that reliance on Wi-Fi itself increases anticipated vulnerability under SIM-binding requirements. Wi-Fi intensity was also included in regression models predicting the expected negative impact. The regression results show that while Wi-Fi usage is nearly universal among SMBs, vulnerability to disruption is not driven simply by being internet-connected once web dependency, multi-device use, and API integration are controlled for ($p > 0.1$). Instead, risk is associated with how messaging is embedded into workflows — particularly through web interfaces, shared access, and API automation. In other words, while Wi-Fi use shows that messaging is internet-native and continuous, but disruption risk arises from authentication structure layered on top of these workflows, which have been discussed below.

Use of Web Versions of Messaging Apps

Mobile phones are only one part of the operational picture. When asked specifically whether they use web or desktop versions of messaging apps for business purposes, 87 percent of SMBs reported using the web versions. Web-based access allows businesses to handle multiple conversations efficiently, integrate messaging with other tools, and share responsibility across staff, which respondents agreed in their responses. The reasons cited by the respondents included higher efficiency, improved employee productivity, and greater convenience of usage. Of these 522 respondents, 93 percent said they use these apps on Wi-Fi for more than 6 hours.



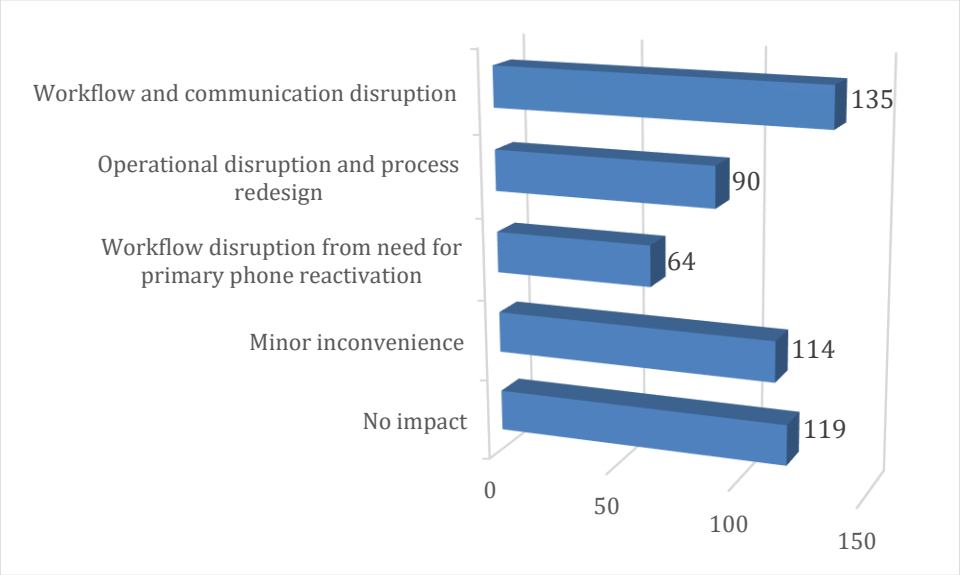
Time for using web versions of messaging apps (n=522 responses for 522 respondents)

A key explanatory variable construct was high web dependency, defined as businesses that reported frequent or essential use of web-based messaging interfaces. The analysis shows that the marginal effect of high web dependency is 0.084, which means these SMBs are around 18 percentage points more likely to anticipate negative

operational impacts from SIM-binding requirements than businesses with low web reliance, even after accounting for differences in size, sector, and location ($p < 0.01$).

Importantly, this effect is substantial in practical terms. Given that baseline concern about disruption is already there, an 18-point increase represents a material escalation of risk and reflects how deeply web-based messaging is embedded in everyday business workflows.

The survey asked businesses to assess the level of disruption they would experience if web sessions were periodically logged out and required re-linking through a SIM-linked primary device. The results show that six-hour web logout mandates could impose friction at the most time-sensitive stages of SMB operations, including customer response windows, order confirmation, staff handovers across shifts, and after-hours support. These are precisely the moments when businesses rely on uninterrupted access to shared or web-based messaging interfaces to maintain continuity. For firms relying on web-based messaging, repeated session expiries via a SIM-linked primary device, creating bottlenecks whenever that device or the employee is unavailable. Ordered logit models confirm this. Increased web dependency significantly increases the probability of falling into higher disruption categories (coefficient ≈ 0.612, $p \approx 0.001$) in the case of strict web logout.

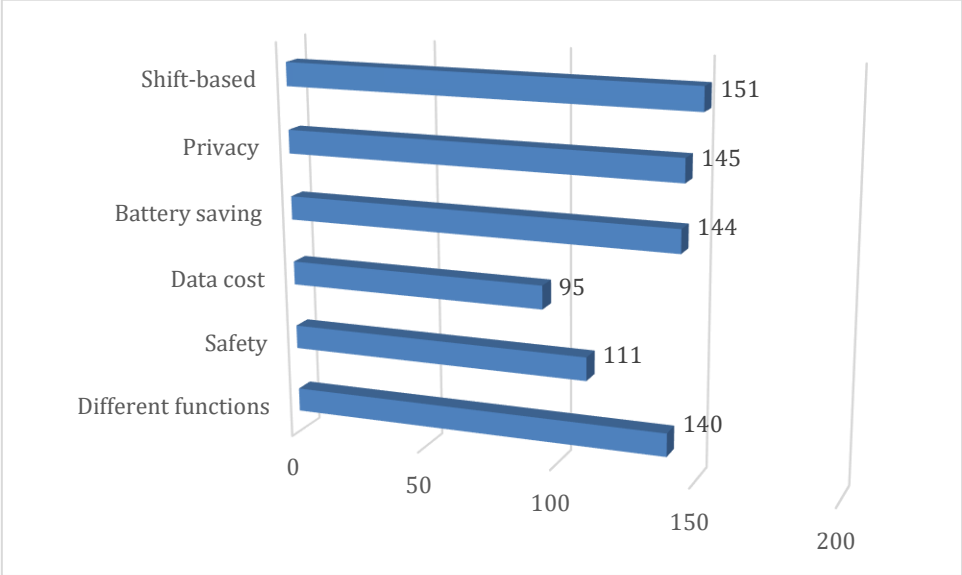


Impact of frequent 6-hour logout of web version (n=522 responses for 522 respondents)

Use of Same Messaging Apps Across Multiple Devices/ SIM Cards

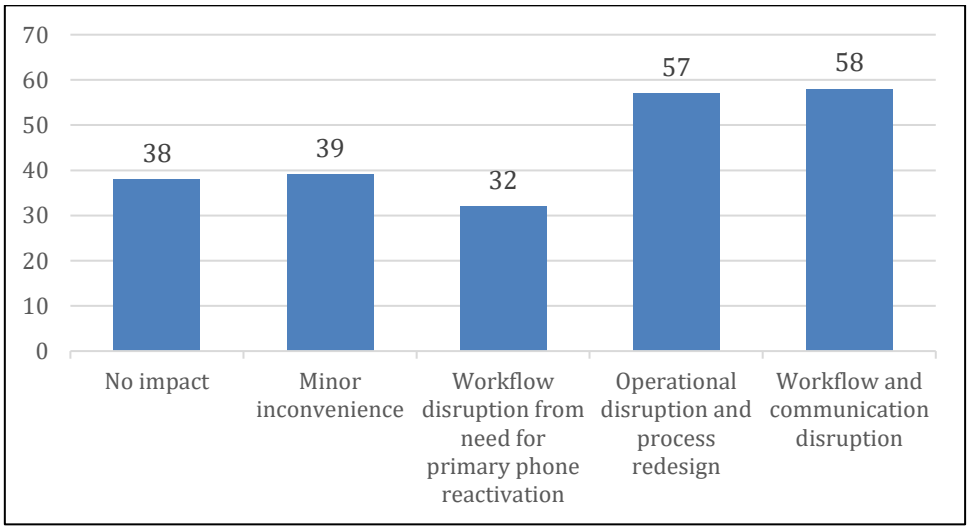
The survey further asked whether businesses use messaging apps across multiple devices or SIMs, such as switching between phones, desktops, tablets, or shared devices depending on shift, role, or location. 37 percent of SMBs reported operating

across multiple devices. This pattern is especially common among businesses with customer-facing teams, rotating staff, or owners who manage operations remotely.



Reasons for operating messaging apps across multiple devices or SIMs (n=786 responses for 212 respondents)

The survey separately examined disruption arising from OTP-based authentication, particularly for businesses operating across multiple devices. Respondents were asked to assess the level of disruption that could by repeated OTP verification when switching devices or re-authenticating sessions. 66 percent of businesses operating across multiple devices reported high disruption from OTP-based verification requirements, with another 17 percent reported they could experience minor disruption.



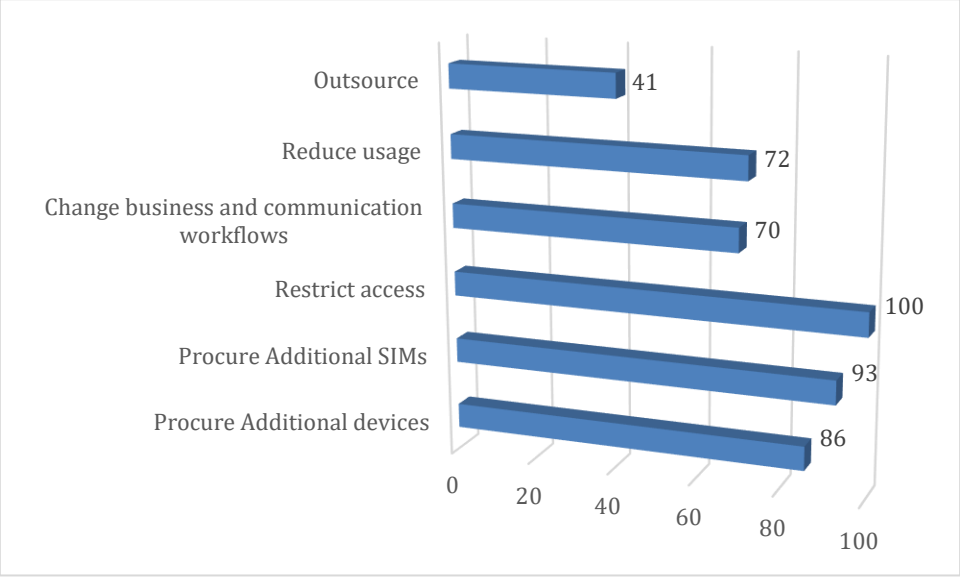
Impact of periodic OTP verification through the primary SIM (n=522 responses for 522 respondents)

These interruptions could accumulate across shifts and among employees, threatening productivity and increasing coordination overhead. Regression results show that multi-device dependence independently increases the likelihood of severe workflow disruption by approximately 15 percentage points, significant at the 5 percent level ($p \approx 0.033$) in the ordered logit model.

Use of same business messaging account by more than one employee or agent

Collaborative usage is widespread. To understand how messaging supports collaborative business activity, the survey explicitly asked whether more than one employee accesses the same messaging account. 35.3 percent of SMBs reported that more than one employee uses the same messaging account for daily operations. This shared-access model is particularly common in customer support, order handling, appointment scheduling, and service coordination. Rather than each employee having a separate number or account, businesses often centralise communication through a single, recognisable channel. This improves customer continuity and allows businesses to respond promptly, regardless of who is on duty.

Regression analysis was conducted to assess whether shared-account usage independently predicts anticipated negative impact under SIM-binding requirements. In the logistic regression model controlling for business size, sector, geographic zone, web dependency, multi-device usage, and API integration, the marginal effect of shared access was small ($p > 0.1$). This indicates that while shared access is associated with disruption descriptively, its impact is largely mediated through deeper workflow characteristics — particularly web-based access and multi-device operation. In other words, it is not the act of sharing alone that drives vulnerability, but the authentication constraints imposed on shared, browser-based, and automated environments.

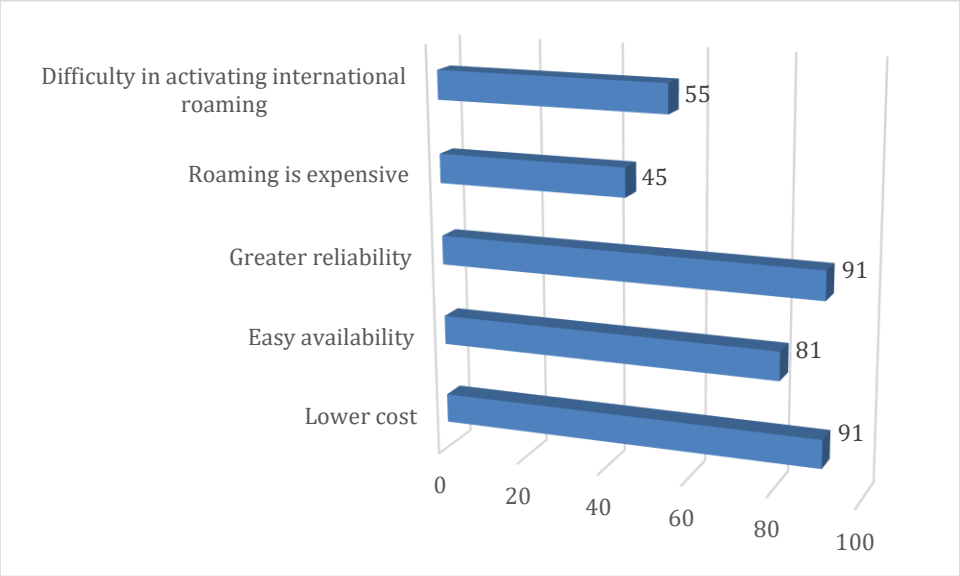


Impact if each employee is required to use a separate SIM-linked device to access messaging apps (n=462 responses for 212 respondents)

However, when examining ordered disruption categories for web logout and OTP re-authentication, shared-access businesses were more likely to fall into medium-to-high disruption groups, with the association statistically significant at conventional levels ($p < 0.05$) in models without API controls. This suggests that shared workflows could amplify disruption when authentication rigidity interacts with employee rotation or shift-based work. This distinction is important: shared access by itself may not automatically generate risk of disruption, but when it does. Still, when dependencies or multi-device operations, it could increase shared access, which by itself may not automatically generate a risk of disruption. Still, when combined with web dependencies or multi-device operations, it could increase that risk. Still, when combined with web dependencies or multi-device operations, it could increase because shared access by itself may not automatically pose a risk of disruption. Still, when combined with web dependency or multi-device operations, it could increase exposure to operational bottlenecks and coordination delays.

International Operations and SIM Availability

The survey also asked businesses whether they use messaging apps while travelling abroad. 20 percent of respondents reported that they or their employees travel outside India and use Wi-Fi or local SIM cards there to operate business messaging apps.



Reasons for using local SIMs while travelling abroad (n=363 responses for 120 respondents)

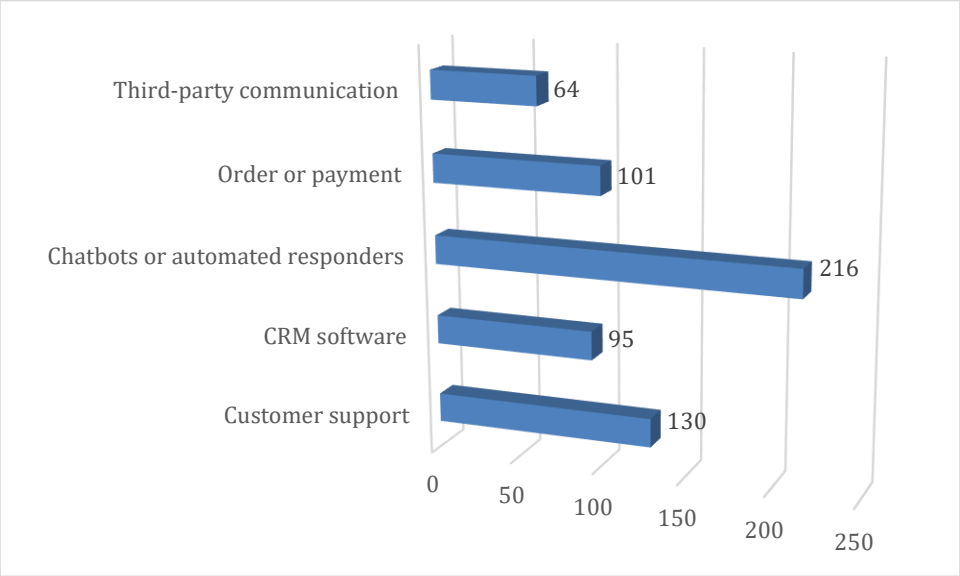
When asked about the types of disruption they could experience if messaging apps cannot be used without the primary Indian SIM being active, the reported impacts varied. Approximately 40 percent (48 of 120) indicated that they would need to procure additional SIMs or devices to maintain continuity. Around 24 percent (29 of 120) anticipated increased operational complexity. In comparison 17 percent (20 of

120) stated they would likely reduce business communications under such constraints, while the rest said they may face some or no impact.

These effects are concentrated among web- and API-dependent firms, suggesting that interruptions in international operations could amplify existing structural risks. Even temporary SIM unavailability could disrupt customer communication, automated systems, and internal coordination, forcing businesses to redesign workflows on the fly.

Use of messaging apps via APIs or cloud-based platforms

The survey asked whether businesses integrate messaging apps with APIs or cloud-based platforms, such as customer relationship management systems, order management tools, or automated response systems. Respondents could indicate whether they did not use APIs at all, experimented occasionally, or relied on them regularly. 53 percent of SMBs reported on APIs or cloud-based integrations for messaging.

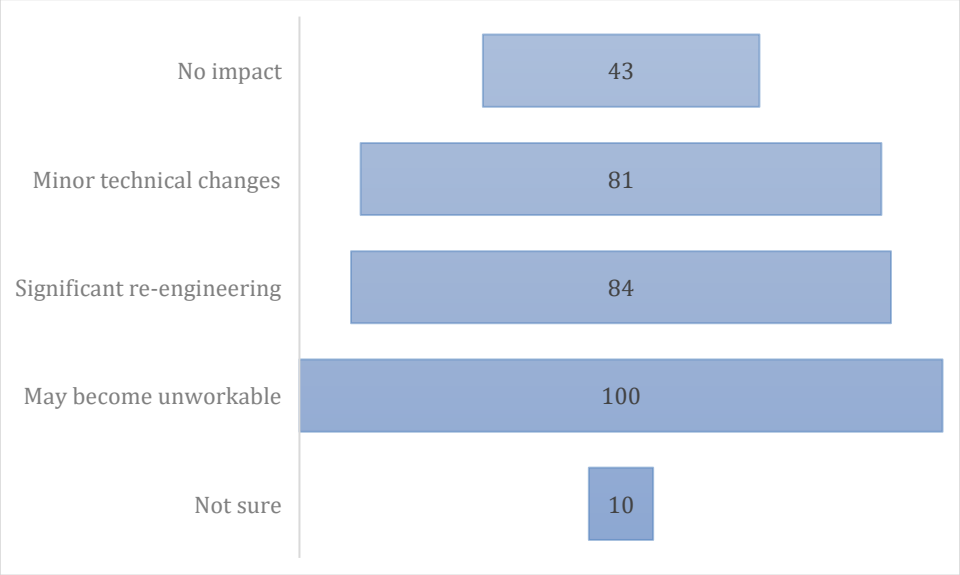


Reasons for using messaging apps via APIs or cloud-based platforms (n=606 responses for 318 respondents)

In the logistic regression model predicting anticipated negative impact, the marginal effect of API dependency is 0.212, indicating that API-dependent businesses are over 20 percentage points more likely to expect significant negative impact than non-API users ($p < 0.001$). This effect is larger than that of web dependency or multi-device usage and remains robust after controlling for business size, sector, and zone. The model's Pseudo R^2 of 0.622 indicates strong explanatory power, lending confidence to the result.

For these businesses, messaging is not merely conversational—it is automated, logged, and integrated into backend systems. Messages support order confirmations, payment reminders, delivery updates, and customer support tickets. This level of integration

significantly increases efficiency but also creates dependencies on persistent access and stable authentication. Thus, any interruption would hamper their operations. Sectoral and size-based differences sharpen these effects. Around 78 percent of e-commerce and platform-based businesses reported high API or web dependency, possible disruption exposure.



Impact of mandatory active SIM presence on API integrations and cloud-based messaging operations (n=318 responses for 318 respondents)

Box 3: Macroeconomic Impact of SIM-Binding–Induced Migration to Paid Messaging Infrastructure

To maintain operational continuity under SIM-binding and session-expiry requirements, many SMBs may be pushed toward paid messaging solutions such as the WhatsApp Business Cloud API. While these platforms do not eliminate authentication requirements, they significantly reduce reliance on repeated web re-linking and primary-device availability by enabling server-based, persistent access. In effect, businesses substitute technical fragility for financial cost, shifting from free app-based workflows to paid infrastructure to remain operational under the new constraints. However, this shift introduces a recurring compliance-driven cost.

Under India's per-message pricing regime, a typical micro-enterprise sending 8,000 business messages per month would incur a blended delivery and platform cost of approximately ₹0.39 per message,[21] reflecting a mix of utility messages and service-provider fees. This translates to a base monthly expense of ₹3,120, which rises to ₹3,682 after 18 percent GST. The annual compliance cost per business would be approximately ₹44,180. For small businesses that previously relied on free app-based messaging, this recurring outlay functions as a *de facto* compliance tax,

[21] The Ultimate Guide to WhatsApp Business API Pricing 2026 (India), Happilee Blog, available at: https://happilee.io/whatsapp-business-api-pricing-2026

imposed not by usage expansion but by the need to remain operational under the new regulatory constraints.

According to available industry estimates, more than 15 million small and medium-sized enterprises in India use WhatsApp Business Solutions.[22] Even if only 10 percent of these SMBs face operational friction under SIM-binding and session-expiry mandates, that would affect approximately 1.5 million businesses, translating into an annual outlay of more than ₹65bn. If 25 percent are affected, the number rises to 3.75 million businesses, implying an annual cost of approximately ₹165bn and corresponding to an annual burden of more than ₹330bn.

Depending on the proportion of affected firms, the potential recurring national outlay could reasonably range between ₹65bn and ₹330bn per year. These figures illustrate that the financial implications of authentication-driven disruption are not marginal. Still, rather, they represent a material, economy-wide operational shift that could affect millions of small enterprises.

The burden is also unevenly distributed. Medium-sized enterprises could face higher absolute costs due to scale and automation intensity, while micro enterprises experience higher relative strain due to limited financial buffers. More importantly, e-commerce and digital services could experience layered financial exposure. Notably, awareness does not significantly mitigate these effects. Even among aware businesses, expected negative financial impact remained high.

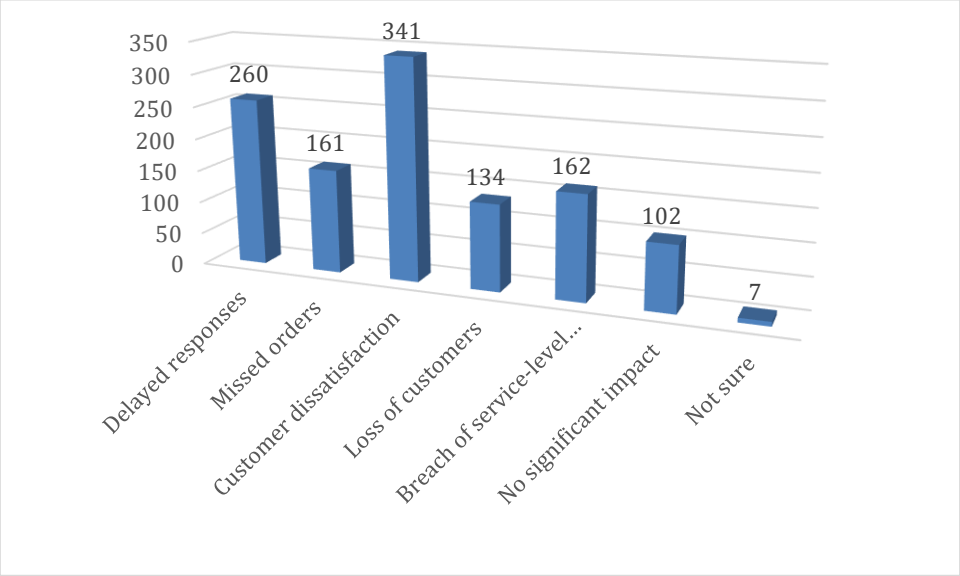
Awareness Versus Operational Reality

The survey also measured awareness of SIM-binding rules among SMBs, asking respondents whether they were unaware, somewhat aware, or fully aware of the requirements. Awareness levels were moderately high at about 60 percent, reflecting media coverage and industry discussions. However, this also implies that approximately 40 percent of firms remain unaware of the proposed requirements. These firms may be particularly vulnerable to sudden implementation effects, as unprepared businesses are less likely to have contingency plans, alternative access mechanisms, or technical workarounds in place. A significant share of the SMB ecosystem may therefore face abrupt operational disruption simply due to informational gaps at the time of enforcement.

However, for those firms which are aware, this did not translate into resilience. While awareness of SIM-binding rules is relatively high among businesses, it does not translate into operational resilience. Businesses reporting full or partial awareness still showed 58-62 percent likelihood of negative impact of the directive, comparable to less-aware firms. Regression analysis confirms that awareness is not a statistically

[22] How WhatsApp Business Delivered the Right Message in Customer Engagement, PitchOnNet, available at: https://www.pitchonnet.com/marketing-moments/how-whatsapp-business-delivered-the-right-message-in-customer-engagement-35994.html

significant mitigating factor once web, multi-device, and API dependencies are taken into account ($p > 0.1$).



Anticipated impact if the operation of messaging apps is disrupted due to SIM-binding requirements (n=1167 responses for 600 respondents)

This gap reflects the limits of informational interventions. Operational constraints such as the need for continuous web access, shared device usage, and automated messaging cannot be resolved through awareness alone. Multi-device and API-dependent businesses would remain exposed regardless of their familiarity with regulatory requirements. Internationally active firms further illustrate this disconnect most clearly. Even with awareness, SIM unavailability during foreign travel could lead to costly disruptions and workflow redesign, underscoring those structural dependencies, not knowledge gaps, drive vulnerability.

Business Size, Sector, Geographical implications, and Workforce Configuration

The survey collected information on business size and sector, analysis of how dependency and disruption vary across firm types. Business size strongly conditions exposure to disruption. Micro enterprises (<5 employees) reported around 40 percent likelihood of negative impact, while small enterprises (6–50 employees) showed over 90 percent web dependency and substantially higher disruption expectations. Medium-sized firms (51+ employees) may exhibit near-universal reliance on the web, leading to consistently high disruption probabilities.

Sectoral differences are also pronounced. Approximately 78 percent of e-commerce and platform businesses rely heavily on API integrations, and around 70 percent are likely to experience significant disruption under SIM-binding scenarios. These businesses depend on persistent messaging access for order processing, logistics coordination, and customer support.

Because these platforms operate through interconnected networks of vendors, delivery partners, warehouse operators, gig workers, and end customers, disruption would not remain confined to the business itself. Delays in authentication or forced logouts can interrupt order confirmations, dispatch instructions, last-mile delivery coordination, and grievance redressal.

Box 4: Economic Impact of Authentication and Forced Logouts for Small Sellers

For small sellers operating on marketplaces, even short interruptions can lead to cancelled orders, payment delays, and reputational harm. Using Indian marketplace data, major platforms like Amazon India have seen peak order volumes of around 18,000 per minute during sales.[23]

Reliance's JioMart quick commerce reported approximately 1.6 million daily orders by the end of Dec 2025,[24] translating to around 1,111 orders/minute. Assuming that everyday volumes across marketplaces likely average 1,500 orders per minute across all sellers. A 5-minute outage could therefore mean around 7,500 orders not processed, which at an assumed order value of ₹1,000 translates to around ₹75 lakhs of gross merchandise value being delayed in 5 minutes. Even for smaller sellers capturing a fraction of that minute-by-minute volume, the missed sales, cancellations, and payment timing delays can materially impact cash flow and reputational scores in seller rating systems. For drivers and gig workers, it can translate into idle time and lost earnings.

At the consumer end, breakdowns in real-time communication can result in non-fulfilment of orders and thus reduce trust. In effect, disruption in platform-dependent SMBs can create ripple effects across supply chains, amplifying economic and welfare impacts beyond the immediate enterprise.

Further, 65 percent of SMBs share messaging accounts among employees, a model that enhances collaboration but becomes fragile under SIM-binding enforcement. Firms using shared access models are significantly more likely to fall into medium-to-high disruption categories ($p < 0.01$), highlighting the trade-off between operational efficiency and authentication rigidity.

Geographic location does not materially insulate businesses from disruption. Zone-level analysis shows that 55–60 percent of SMBs across all regions anticipate negative impacts, and regression models find no statistically significant zone effects after

[23] Amazon Prime Day breaks records with 18,000 orders per minute in India, Business Standard, available at: https://www.business-standard.com/amp/companies/news/amazon-prime-day-india-orders-hit-record-18000-per-minute-125072101237_1.html

[24] Reliance's JioMart hits 1.6 million daily orders, claims to be second-largest qcomm player in India, The Economic Times, available at: https://m.economictimes.com/tech/technology/reliances-jiomart-hits-1-6-million-daily-orders-claims-to-be-second-highest-qcomm-player-in-india/articleshow/126599996.cms

accounting for workflow dependencies. This suggests that the risk is systemic rather than location specific. Even businesses operating in well-connected urban regions face similar vulnerabilities, indicating that digital infrastructure alone cannot offset authentication-driven constraints embedded in platform design.

Conclusion and Recommendations

Policymakers face the challenge of balancing robust digital security with the realities of India's rapidly expanding and diverse digital ecosystem. The widespread use of smartphones, multiple devices, and shared accounts means that strict adherence to continuous SIM-binding, mandatory logouts, and repeated authentication can create significant friction for users, businesses, and households.

Survey evidence shows that multi-device and multi-SIM workflows are essential for communication, education, financial transactions, and continuity of work. Nearly two-thirds of users rely on multiple devices or SIMs daily, and household device-sharing is common across urban, semi-urban, and rural areas. These practices help maintain connectivity amid device failure, network disruptions, travel constraints, or economic limitations. Regulatory frameworks that ignore these dynamics risk disruption and exclusion. While the intention behind implementing SIM-binding is to enhance security, compliance, and traceability, rigid enforcement could limit access for women, seniors, and children, disrupt education and work, and impede international mobility. Given these trade-offs, it is important to carefully assess whether the proposed measures are proportionate to the risks they seek to address and to explore alternative approaches that can strengthen security without undermining accessibility and usability.

Recommendations

Conduct Comprehensive Regulatory, Technical, and Privacy Impact Assessments: Before implementing, evaluate the regulatory, technical, and privacy implications. A regulatory impact assessment should clarify the legal basis, scope, and proportionality of the intervention. A technical impact assessment should test feasibility, interoperability, and enforcement challenges across devices, operating systems, and platforms. A regulatory sandbox framework or a full-scale rollout could complement this process. Such sandbox pilots should systematically evaluate key technical design variables, including session expiry duration, re-authentication frequency, and device-persistence configurations.

In particular, controlled testing of automatic logout mechanisms for web-based and desktop-based sessions across different time intervals—such as six-hour, twelve-hour, and twenty-four-hour windows—as well as activity-based sessions, could help generate empirical evidence. Comparative assessment of these approaches can

quantify the trade-offs between fraud prevention and potential workflow disruption, enabling regulators to calibrate authentication requirements based on measured outcomes rather than uniform assumptions.

A privacy impact assessment should examine risks to user data, consent, and personal information, ensuring safeguards are in place. Conducting these assessments upfront would allow evidence-based policymaking, reduce unintended disruptions, and align interventions with user rights and operational realities.

In addition, where security benefits are cited as justification for such measures.[25] The underlying empirical evidence should be made public. If studies assessing the anticipated reduction in cyber fraud, financial scams, or national security risks have been conducted, these should be disclosed to enable informed discussions. In the absence of such published evidence, independent impact evaluations should be commissioned to assess whether proposed authentication mandates can meaningfully reduce cybercrime, without unnecessarily burdening consumers and SMBs.

As part of this process, the specific relevance of SIM-binding in addressing identified threat vectors should be transparently examined and demonstrated. Alternative mechanisms should also be comparatively evaluated to determine the most proportionate and effective intervention. Such structured comparison could ensure that regulatory choices are guided by measurable risk reduction rather than uniform compliance assumptions.

Prioritising Risk-Based, Evidence-Driven Security Measures: Security interventions should focus on addressing real threats without creating unnecessary friction for users. Security interventions should focus on addressing real threats without creating unnecessary friction for users. This assessment should account not only for the immediate inconvenience of actions such as entering a one-time password, but also for indirect workflow effects—including session interruptions, paused transactions, coordination delays, and the need to restart authentication processes across devices.

Messaging platforms already employ multiple security mechanisms—including two-factor authentication, AI-driven fraud detection, and behavioural monitoring—that demonstrate tailored, data-driven approaches that can mitigate risks effectively. By contrast, continuous SIM-based verification, repeated logins, and mandatory authentication can disproportionately burden users, particularly those with multiple devices or shared accounts, a common practice in urban, semi-urban, and rural India.

Importantly, this need not be framed as a trade-off between security and convenience; regulatory design can strengthen authentication safeguards while remaining responsive to how people actually access and share digital services.

[25] Linking WhatsApp with SIM Cards Can Stop 'Digital Arrest' Scams: Govt to SC, Trak.in, available at: https://trak.in/stories/linking-whatsapp-with-sim-cards-can-stop-digital-arrest-scams-govt-to-sc/

Rapid enforcement, such as the proposed 90-day implementation timeline, without any prior consultation, can produce fragile technical systems, inconsistent compliance, and high costs with minimal practical benefit. A measured, risk-focused approach that leverages analytics, telecom-assisted monitoring, and adaptive fraud detection can strengthen security while maintaining everyday usability.

Involve Stakeholders and Educate Consumers: Effective security interventions require input from multiple stakeholders, including app developers, cybersecurity experts, technical specialists, and civil society. Their guidance ensures that interventions are proportionate, technically feasible, and user-centric. In parallel, transparency around proposed regulatory changes—including how authentication models may affect account access, device sharing, and data handling practices—can help users understand potential implications for privacy, access continuity, and shared-device arrangements. Educational initiatives, grievance redressal mechanisms, and trust-building efforts complement technical safeguards, fostering a culture of security without unnecessarily disrupting digital routines.

Establish Clear Regulatory Boundaries and Consultation Mechanisms: Regulatory clarity is essential. Mobile number-based identification alone does not justify subjecting internet-based platforms to telecom regulations. Expanding regulatory authority in this way risks overstepping legislative mandates, introducing enforcement ambiguities, and chilling innovation. The definition of TIUEs, for instance, could inadvertently encompass platforms whose primary purpose is not communication.[26]

Mandatory public consultation should precede sweeping measures such as SIM binding. Current directives assume seamless SIM access across operating systems, an assumption that conflicts with existing iOS and Android privacy restrictions. Structured discussions enable evaluation of technical feasibility, alternative approaches, and trade-offs, preventing regulations from imposing disproportionate operational and financial burdens on users, businesses, and service providers.

Adopt Proportionate, Low-Friction Regulatory Mechanisms: Regulatory interventions must adhere to the principle of proportionality. Broad, uniform requirements like continuous SIM verification increase friction, elevate costs, and risk excluding vulnerable groups, including women, children, and low-income households who rely on shared devices or multiple SIMs.

Targeted, risk-based models offer a more flexible and effective approach. Industry and technical research on modern authentication systems emphasise adaptive, risk-based authentication approaches in which contextual signals—such as device attributes,

[26] The Cost of Telecom Cyber Security: Impact of the 2025 Amendment Rules on Consumers and Small and Medium Businesses, CUTS CCIER, available at: https://cuts-ccier.org/pdf/the-cost-of-telecom-cyber-securit-impact-of-the-2025-amendment-rules-on-consumers-and-small-and-medium-businesses.pdf

geolocation patterns, network characteristics, and behavioural indicators—are analysed to calculate risk scores and dynamically tailor verification requirements.[27] Such models, widely discussed in contemporary risk-based authentication literature, aim to balance security needs with usability by incorporating real-time anomaly detection, device telemetry, and contextual decision-making into the authentication process. By analysing SIM age, usage patterns, KYC history, and unusual activity, telecom operators can generate a composite risk index for applications.[28]

Platforms can then respond proportionately, preserving multi-device, multi-SIM, and shared-account usage, which are crucial for education, work, and communication. When verification is necessary, low-friction solutions such as background APIs like GSMA Connect (CAMARA) enable silent, real-time checks that enhance security without disrupting users.[29]

For example, CAMARA-aligned Number Verification APIs allow applications to confirm that the phone number belongs to the device accessing a service by querying mobile network operator infrastructure in the background, without requiring one-time passwords or manual input, thereby reducing friction and improving both security and user experience. Other related APIs can detect SIM swaps, validate identity attributes, or subscribe to device connectivity status, providing a suite of tools that can be used.[30] Such adaptive, targeted measures maintain accessibility, reduce costs, and preserve usability, balancing protection with convenience.

Strengthen Governance, Consultation, and Strategic Oversight: The SIM-binding debate highlights the need for principled, evidence-based policymaking that protects users without overregulation. To prevent unintended consequences, India should pause the current implementation timeline and initiate formal consultations under the Telecom Cybersecurity Rules. A multi-stakeholder technical working group, including industry representatives, independent security experts, consumer groups, and civil society, should explore technology-neutral, risk-informed solutions aligned with real-world user behaviour.

Given the rapid pace of technological innovation, regulatory approaches should avoid hardcoding specific technical requirements that may quickly become outdated or inadvertently constrain more secure or efficient authentication methods in the future.

---

[27] Davis, J. (2025). Modern authentication methods: Enhancing security and user experience. Journal of Information Systems Engineering and Management, 10(60s). https://doi.org/10.52783/jisem.v10i60s.13076
Sulochana, G. G. D., & De Silva, D. I. (2025). Blockchain–AI–Geolocation Integrated Architecture for Mobile Identity and OTP Verification. Future Internet, 17(12), 534. https://doi.org/10.3390/fi17120534

[28] Impact of SIM Binding on Social Media, MediaNama (Event Report, December 2025), available at: https://www.medianama.com/wp-content/uploads/2025/12/Event-Report_-Impact-of-SIM-Binding-on-Social-Media.pdf

[29] Ibid

[30] Impact of Number Verification API, Open Gateway by Telefónica (Documentation, 2026), available at: https://developers.opengateway.telefonica.com/docs/numberverification

In parallel, a comprehensive anti-fraud strategy should be developed. Strengthening SIM KYC processes at the point of issuance can mitigate vulnerabilities at the root, reducing the necessity for sweeping downstream mandates such as SIM binding.[31] Proper verification during SIM allocation can better address misuse risks. Such measures are likely to be more effective and less disruptive than shifting ongoing authentication burdens onto end consumers and SMBs, many of whom operate with limited compliance capacity.

Ultimately, India's goal must be to achieve robust digital security without undermining usability or innovation. Clear regulatory boundaries, structured consultation, targeted risk-based interventions, transparency, and proportionality are key. Security measures should enhance accessibility, inclusion, and innovation rather than impose administrative convenience at the expense of social and economic participation.

[31] Ibid

CUTS International

D-217, Bhaskar Marg, Bani Park, Jaipur 302 016, India
Ph: 91.141.228 2821, Fax: 91.141.228 2485
Email: cuts1@cuts.org, Website: www.cuts-international.org

Also at Delhi, Kolkata and Chittorgarh (India); Lusaka (Zambia); Nairobi (Kenya); Accra (Ghana); Hanoi (Vietnam); Geneva (Switzerland) and Washington DC (USA).