Consumer Protection

Fear of privacy violations

Privacy violations occur when personal data, such as financial records, location information, or digital communication, is breached or misused without their knowledge or consent. **This might involve unauthorized data collection or storage, exposure of sensitive information, or a lack of transparency around how personal data is stored and used.** For many women, privacy concerns are closely related to fears of surveillance, harassment, or reputational damage. Importantly, breaches of privacy not only compromise personal safety but also erode consumer trust in financial institutions, making women more hesitant to adopt or continue using formal financial services.

Why is this barrier important?

This heightened sense of vulnerability can result in self-censorship or withdrawal from digital financial platforms altogether. Even when services are available, women may choose not to use them if they feel their personal information is at risk. In turn, this limits their ability to access digital loans, mobile money, or savings tools, exacerbating financial exclusion. Building strong data protection safeguards, educating users on their rights, and designing inclusive privacy practices are critical steps mitigating these violations, and ensuring that digital inclusion doesn't come at the cost of personal safety.

Connected Barriers

Policy & Regulation
Lack of gender-intentional NFIS

Digital & Physical Infrastructure
Poor internet & mobile connectivity
Lack of female agents
Unreliable payment system & network

Institutional Norms & Practices
Lack of strategic focus on women customers
Low digital capabiltiy of financial institutions

Consumer Protection
Difficulty resolving complaints

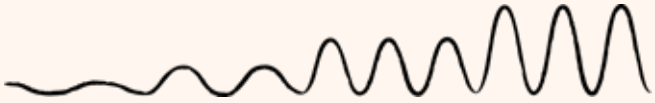
Entry & Capability Barriers
Low digital financial capability
Limited personal exposure to DFS

Product & Market Design
Poor understanding of women's financial needs

Most Relevant Segments

1	2	3	4
Excluded, marginalized	Excluded, high potential	Included, underserved	Included, Not underserved

Customer Journey Relevance



Phase 1:	*Phase 2:*	*Phase 3:*	*Phase 4:*
Account Ownership	Basic Account Usage	Active Account Usage	Economic Empowerment

Key evidence relevant to this barrier

Lack of password protection leaves accounts vulnerable.

Evidence points to low data security in many contexts, in part because of a lack of awareness among customers of strategies to protect privacy and account security. Privacy violations – both real and perceived – contribute to unwillingness to use digital financial services, especially among women.

- In low- and middle-income economies, only 60% of mobile phone owners have a password on their mobile phones, and more men than women mobile phone owners have passwords on their devices. Lack of password protection leaves accounts vulnerable to access by family members or thieves. While most providers require a PIN for transactions, weak phone security still undermines confidence in mobile money. (World Bank, 2025)
- Research in India revealed that concerns about their data and security can lead women to curtail their use of different services and self-censor their behavior. Women might also lack knowledge of how to safeguard their personal data and rely on male family members and more educated people for advice on how to protect their photos, social media messages, etc. (Dalberg, 2021)

Customers, especially women, place a high value on privacy.

Data suggest that women and men differ in their value of privacy, with women placing a higher emphasis on the need for privacy protection than men. This indicates that financial actors could and should invest in both privacy protection and education and awareness-building.

- Research shows that women often have distinct financial preferences, with many placing a particularly high value on privacy in their financial services. (Women's World Banking, 2024)
- Interviews with low and middle-income men and women suggest that women see data use violations far differently than men do, and that DFS providers should take this into account. Women's concerns parallel the challenges and threats they encounter in their physical lives, such as location tracking and sexual harassment. (Collins, 2021)
- A 2020 study offered 171 low-income customers in Kibera a loan that required some level of data-sharing. 71 (42%) declined, of which half cited privacy concerns. Of those who did take the loan, 52% chose a more expensive option that offered privacy protections. While these data were not sex-disaggregated, they indicate that low-income customers were willing to pay a premium for greater protection of their personal data in digital loan services. (Fernandez Vidal, 2020)

Protecting customer privacy requires clear communication, customer empowerment, and accountable response systems that build trust and resilience.

Institutions should align data protection policies with national and international standards while ensuring they are transparent and accessible in local languages, and invest in customer education that equips women to manage their privacy and digital safety independently. These prevention efforts must be complemented by timely disclosure, accessible support, and effective resolution mechanisms when privacy violations do occur. Recommendations include:

- Strengthen data protection policies and compliance by aligning with national and international data protection standards in creating clear, customer-centered privacy policies. These policies must explain in simple, local languages how personal data is collected, stored, used, and shared. Practical checklists and internal audits can help to ensure compliance and accountability.
- Invest in customer education on privacy rights and digital safety through digital capability sessions that teach women how to

Key evidence relevant to this barrier

adjust privacy settings, securely use mobile phones, and protect sensitive information such as photos, PINs, and messages. Because many women often rely on male relatives for guidance, financial service providers (FSP) should embed practical support directly through in-app tutorials, SMS tips, or dedicated helplines that address common privacy concerns (e.g., preventing location tracking, recognizing fraud attempts). These measures empower women to manage their digital security independently, reduce reliance on others, and build confidence in using financial services.

- Develop a strategy for customer engagement and resolution of issues following privacy violations or breaches. This should include transparent disclosure of the breach, clear guidance to customers on protective steps they can take (e.g., changing PINs or passwords), and accessible channels for support. In addition, FSPs should establish redress mechanisms, such as compensation for losses or expedited account recovery, to rebuild trust and demonstrate accountability.
- Advocate for the development of a robust digital ID ecosystem. This could help increase the user base quickly through meaningful incentives, embed strong privacy protections that give citizens control over their data, and expand use cases so that the ID becomes an essential and valuable tool in daily life.