Consumer Protection

Increased exposure to frauds and scams

This barrier refers to deceptive third-party practices that target customers through various channels, including mobile banking, mobile money, fintech apps, and traditional banking systems. **These can include phishing attempts, fraudulent credit schemes, unauthorized transactions, or scams carried out by agents and third parties.**

Why is this barrier important?

For financial services providers (FSP), fraud and scams present both operational and reputational risks. Customers who experience fraud often lose trust in financial institutions and may withdraw from using formal financial services altogether. Institutions face complaints, reputational damage, and regulatory scrutiny, while customers bear the direct financial and emotional costs of fraud. Women, who may already face barriers such as lower digital literacy, limited mobility, or shared phone use, are often less equipped to detect and recover from fraud. When scams occur, the consequences go beyond financial loss; they create deep mistrust in digital and formal financial systems, discouraging women from adopting or consistently using financial products. Without robust protections, transparent redress systems, and proactive education campaigns, women are likely to disengage, slowing progress toward financial inclusion.

Connected Barriers

Consumer Protection

Difficulty resolving complaints
Fear of making mistakes
Non-transparent product information
Fear of privacy violations
Predatory lending
Overcharging

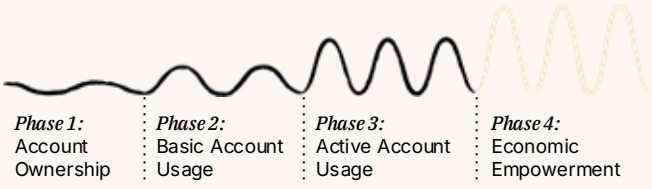
Policy & Regulation

Lack of gender-intentional NFIS

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

Global trends suggest an uptick in fraud complaints.

Especially against the landscape of rising digitization and expansion of financial services, increases in fraud are widespread. These include phishing scams, opaque costs, and network issues, and are compounded by insufficient or dissatisfactory recourse mechanisms. This results in lack of trust in financial institutions and systems and suspicion of digital devices, transactions, and services.

- Qualitative interviews with FSPs reveal that fraud and scams are one of the most significant barriers facing women customers, contributing to a lack of trust in financial products and services. (Women's World Banking, 2025)
- Rapid digitization has led to increased consumer risks, including fraud, data misuse, and inadequate recourse mechanisms. Specific examples of fraud include SIM swap fraud and mobile app fraud. (CGAP, 2024)
- According to the KPMG Global Banking Scam Survey 2025, 60% of survey respondents reported increased scam-related complaints. Most common complaints included dissatisfaction with reimbursement decisions, frustration with transaction friction, and feeling banks could do more to protect consumers. (KPMG, 2025)
- National surveys in Côte d'Ivoire and Senegal reveal that 88% of DFS users have been exposed to some form of risk, including receiving scam or fraudulent messages, not being informed of the cost of the service, and experiencing poor network issues. Financial losses as a result of these risks were reported by 40% of users in Côte d'Ivoire and 32% in Senegal. (CGAP, 2024)
- The Nigeria Consumer Protection in Digital Finance Survey (2021) finds that 26% of digital finance customers cited "phishing by phone or SMS" as a common challenge. This is the third most cited challenge, out of nine, among customers. (MicroSave Consulting, 2022)
- In Kenya, respondents cite "fraud/attempted fraud" by mobile money providers (26.6% of respondents), mobile banking (9.9% of respondents), and mobile apps (4.7% of respondents) as major challenges. (FinAccess, 2024)
- In Nigeria, fraud and security risks are significant concerns as online payments continue to grow. (Imhodibie, 2025)
- Nyoni et al. (2024) writes that the financial sector is the most vulnerable industry in South Africa to data breaches. The South African Banking and Risk Information Centre confirms that in 2018, the banking sector incurred over R260 million in gross losses due to cyber incidents.
- Leaders of an agri-insurance firm in Kenya cite repeated scams targeting farmers as the primary barrier to product adoption, leading to widespread mistrust among both male and female customers. (Women's World Banking, 2026)

To strengthen trust and combat fraud, some providers and financial institutions have invested in education campaigns, AI detection schemes, and recovery options.

Successful efforts adopt a proactive, multi-layered approach to fraud prevention and consumer protection, including real-time detection and response capabilities, as well as customer awareness-building and digital safety education, including community-based ambassador programs and the integration of scam prevention into onboarding and ongoing engagement.

- Some banks have implemented various initiatives to educate customers about scams, including social media campaigns, scam alerts via emails or SMS, educational webinars, and interactive tools on websites or mobile apps. (KPMG, 2025)

Key evidence relevant to this barrier

- A 2025 survey of financial services providers finds that 45% of institutions are proactively implementing mitigation strategies against fraud and scams, including AI-based fraud detection systems and customer education efforts. (Women's World Banking, 2025)
- In Indonesia, a fintech company has implemented fraud prevention strategies, including internal audits and whistleblower systems, to combat agent-related fraud and build trust among rural women clients. (Women's World Banking, 2026)
- In Mexico, fraud and scams are common forms of extortion and fraudulent credit schemes. One fintech company in Mexico responds to fraud cases by advising customers to contact them directly and offering flexible repayment options, such as interest-free installments or payment deferrals, to help affected consumers recover and rebuild trust. (Women's World Banking, 2026)

Combating digital fraud and technology-facilitated abuse requires a proactive, system-wide approach.

FSPs should invest in artificial intelligence and machine learning (AI/ML) tools to detect fraud in real time, while integrating behavioral nudges and safeguards to prevent scams before they occur. These measures should be complemented by sustained customer education and community-based awareness efforts, alongside strong institutional protocols and partnerships with law enforcement to identify, escalate, and respond to cases of fraud and digital abuse effectively. Recommendations include:

- Invest in AI/ML tools to detect unusual patterns and identify emerging fraud schemes in real time. These measures can enable FSPs to identify fraudulent activity early and spot systemic threats to prevent scams from spreading across institutions.
- Introduce real-time customer prompts into digital transaction processes (e.g., "Is this person known to you?") to encourage customer reflection before finalizing payments. Behavioral "nudges" and simple confirmation messages can reduce impulsive responses to scams.
- Strengthen customer awareness and digital literacy through ambassador programs where trained community members, especially women, raise awareness about common scams and digital safety practices. FSPs can incorporate scam education into onboarding, product usage tutorials, and ongoing engagement campaigns.
- Roll out two-factor authentication for higher-value or high-risk transactions to reduce fraud exposure, and develop "trusted sender" verification systems, allowing customers to pre-approve or flag safe contacts for recurring transactions. These safeguards make it harder for fraudsters to access accounts or impersonate trusted contacts.
- Collaborate and establish referral systems with law enforcement to escalate cases of technology-facilitated abuse. With customer consent, FSPs can document repeated abusive transactions and refer them directly to specialized police units, ensuring quicker intervention and reducing the burden on victim-survivors. To support this, staff should be trained to identify patterns of digital abuse and follow protocols that safeguard customers' privacy and safety.
- Incorporate consumer protection training as part of service delivery to strengthen safeguards against fraud and scams. These trainings should directly address common doubts individuals may have regarding their identity and data protection, helping customers feel secure and informed when engaging with financial services.