White Paper

Privacy and security for women-led SMBs in digital financial services



GSMA Mobile for Development

M4D

The GSMA is a global organisation unifying the mobile ecosystem to discover, develop and deliver innovation foundational to positive business environments and societal change. Our vision is to unlock the full power of connectivity so that people, industry, and society thrive.

Representing mobile operators and organisations across the mobile ecosystem and adjacent industries, the GSMA delivers for its members across three broad pillars: Connectivity for Good, Industry Services and Solutions, and Outreach. This activity includes advancing policy, tackling today's biggest societal challenges, underpinning the technology and interoperability that make mobile work, and providing the world's largest platform to convene the mobile ecosystem at the MWC and M360 series of events.

We invite you to find out more at www.gsma.com

Follow the GSMA on X: @GSMA

GSMA Mobile Money

The GSMA's Mobile Money programme works to accelerate the development of the mobile money ecosystem for the underserved.

For more information, please contact us:

www.gsma.com/mobilemoney

mobilemoney@gsma.com

Visa is a world leader in digital payments, facilitating transactions between consumers, merchants, financial institutions, and government entities across more than 200 countries and territories. The "Digital Finance for All" (DFA) initiative, a Visa-funded partnership between Visa and the GSMA Mobile for Development Foundation, is committed to advancing sustainable growth. The DFA programme aims to enable individuals and small and micro businesses (SMBs) in low and middle-income countries (LMICs) with digital financial services and financial education to bolster financial inclusion.

Authors:

Panos Loukos, GSMA
Dalberg Research Limited

Acknowledgements

We extend our sincere appreciation to Visa for collaborating with the GSMA on this study and to Dalberg Research Limited for spearheading its implementation. We are also grateful to the many stakeholders, including development agencies, consumer organisations, mobile network operators, regulators, digital financial service providers, microfinance institutions and fintechs, that generously shared their time, insights and expertise and enriched this work: Financial Sector Deepening (FSD) Kenya, Consultative Group to Assist the Poor (CGAP), United Nations Capital Development Fund (UNCDF), International Finance Corporation (IFC), World Food Programme (WFP), Kenya Consumer Organisation, Safaricom Limited, Central Bank of Kenya, Jumo World, ECLOF Kenya, Onafriq, Mukuru Limited, Numida Technologies Limited, OYE, Tala Mobile Kenya Limited and Juhudi Kilimo Company Limited.

Published: December 2025

Contents

Executive summary	**2**
1. Introduction	**4**
Scope and research objectives	8
Target audience	8
Methodology	8
2. Perceptions and expectations of DFS privacy and security	**9**
Perceptions of privacy and security when accessing DFS	9
Expectations of privacy and security when accessing DFS	10
The gap between perceptions and expectations	12
3. Privacy and security in a DFS ecosystem: key actors and solutions	**13**
Key sector actors and their role in privacy and security	13
A taxonomy of privacy and security solutions for DFS	15
4. Women-led SMBs and DFS: privacy and security considerations	**17**
5. Conclusion	**19**

Executive summary

Small and micro businesses (SMBs) are the backbone of economic growth and resilience across low- and middle-income countries (LMICs). They provide most of the employment opportunities, nurture entrepreneurial ecosystems and drive innovation at the local level. Women-led SMBs form a critical part of this sector, providing livelihoods and enabling inclusive economic participation. Yet, despite their contributions, women entrepreneurs face persistent barriers to accessing and fully benefitting from digital financial services (DFS).

DFS, which range from mobile money to digital credit, savings and payments, have become indispensable tools for SMBs by offering scalable, affordable and accessible financial solutions. In markets such as Kenya, mobile money platforms like Safaricom's M-PESA, have transformed how small businesses transact, save and grow. For women entrepreneurs, however, adoption and sustained use of DFS is shaped not only by product availability but also by perceptions of privacy and security. Since financial services are inherently based on trust, women's willingness to engage depends on how safe they feel about their data, transactions and identities when using DFS.

This white paper explores the perceptions, expectations and lived experiences of women-led SMBs regarding privacy and security in DFS. Drawing on 18 key informant interviews (KIIs) in Kenya, one of the world's most dynamic DFS markets, and consumer insights from Visa's Consumer Empowerment Studies in Kenya and across Central and Eastern Europe, Middle East and Africa (CEMEA), the findings highlight how privacy and security concerns directly influence adoption, use and trust of DFS.

Key findings

1. **Perceptions influence adoption.** Women entrepreneurs often have cautious or skeptical views of DFS, due to low digital literacy and stories of fraud and unauthorised data sharing. In Kenya, for example, only 11% of consumers fully understand how their data is used and 85% report concerns about unauthorised access. These perceptions often discourage uptake beyond basic services.[1]
2. **Customer loyalty depends on meeting expectations.** Women-led SMBs expect providers to deliver comprehensive data protection, transparency and accessible grievance mechanisms. More than 79% of Kenyan consumers consider transparent communication about data use a decisive factor in continuing to share digital data.[2] Meeting these expectations is not optional – it determines whether SMBs will engage more deeply with DFS, such as using it for savings, loans or digital business tools.
3. **There is a persistent gap between perceptions and expectations**. Women entrepreneurs expect DFS to be safe, transparent and user-friendly. Yet, many still perceive products as risky, opaque or socially compromising. This gap causes many to restrict their usage to basic person-to-person (P2P) transfers, avoiding higher-value services such as digital credit, savings or business analytics. The result is missed opportunities – women's businesses remain under-digitalised and DFS providers lose out on a loyal and expanding customer base. This mismatch fuels mistrust, limits adoption, stunts business growth and prevents providers from cultivating a loyal customer base.
4. **Privacy and security are ecosystem-wide issues.** Multiple actors, including DFS providers, fintechs, banks, regulators and consumer associations, play a role in privacy and security. While many providers deploy tools such as PINs, one-time passwords, biometric authentication and fraud alerts, gaps remain in communication, education and aligning with the lived realities of women entrepreneurs.

1 Visa. (2024). How Empowering Consumers Promotes a Trusted Digital Economy. Visa Consumer Empowerment Study for Kenya. Unpublished report.
2 Ibid.

Implications

Privacy and security are not just about compliance or technical safeguards – they are also about building trust. For women-led SMBs, trust in DFS equates to business stability, personal safety and financial autonomy. For providers, it represents a pathway to scale, deeper engagement and long-term customer loyalty. The analysis underscores a simple but critical point: **closing the perception-expectation gap is essential to unlock the full potential of DFS for women-led SMBs**. This requires transparent and user-centred products that respond to women's unique user needs and business contexts.

Next steps

This white paper introduces a **taxonomy of privacy and security solutions** to describe how different DFS ecosystem actors are addressing women's privacy and security needs. Solutions are grouped into five categories:

1) Product design features, such as encryption, PIN and biometric authentication

2) Consent and data governance protocols, such as granular consent prompts, opt-in data sharing and transparent terms of service

3) User education and digital literacy delivered via digital and offline channels

4) Dispute resolution mechanisms, such as call centres, in-app reports and ombudsman services

5) Collaborative standards and industry governance through cross-sector coalitions

This taxonomy provides a structure to understand existing efforts and highlight where solutions may fall short of women-led SMBs' expectations.

Building on this analysis, the final chapter presents considerations for DFS providers and other ecosystem actors to close the perception-expectation gap. These include designing with women's lived realities in mind, making security features visible and comprehensible and providing accessible channels for dispute resolution. By centring the voices and experiences of women entrepreneurs, this white paper underscores that privacy and security are not peripheral concerns, but rather enable trust, participation and empowerment in the digital economy. Ensuring that women-led SMBs can engage confidently with DFS is therefore a commercial imperative and pathway to more inclusive and resilient economies.



1. Introduction

Small and medium enterprises (SMEs) drive economic activity, particularly in low- and middle-income countries (LMICs). The SME sector represents a significant proportion of global businesses, accounting for approximately 90% of all enterprises and contributing more than 50% of employment worldwide.[3] As businesses create economic opportunities for marginalised groups such as women, youth and rural populations, they also promote poverty reduction, gender equality and social inclusion.[4] In Africa, SMEs number around 44 million, contributing up to 80% of employment in some countries and fostering inclusive growth by providing opportunities for these marginalised groups.[5]

Women-led SMEs, which constitute roughly one in three businesses globally, are vital contributors to household livelihoods and community well-being.[6] In LMICs, these are mostly small and micro businesses (SMBs), often operating in informal or semi-formal settings through market stalls, kiosks or home-based ventures, where owners manage various ventures while also balancing household and caregiving responsibilities. Despite their substantial economic contributions, **women entrepreneurs face a considerable financing gap estimated at USD 1.7 trillion globally.**[7] This gap is exacerbated by factors such as low financial literacy, restrictive social norms, cultural inequalities, inadequate financial products and a lack of collateral. These challenges hinder the ability of women-led SMBs to scale, participate in the formal economy and compete in other markets and the digital economy, all of which perpetuate economic inequality.

Digital financial services (DFS) offer the most scalable and accessible solution to address the financing needs of SMBs by providing faster, more affordable and data-driven access to credit and other financial services. DFS platforms, such as those delivered via mobile phones and agent networks, can reach underserved populations in remote areas where there are no brick-and-mortar banks. Services can be accessed anytime and from anywhere with little or no need to travel, greatly improving accessibility. Most DFS providers embrace simple know your customer (KYC) procedures, which lowers barriers to onboarding and provides a flexible solution for informal and unbanked women-led SMBs to enter the financial system.

Importantly, the growth of female DFS agents have advanced digital financial inclusion for women entrepreneurs and other underserved groups. Female agents often provide more approachable and trusted access points for women users, helping to overcome socio-cultural barriers, privacy concerns and gender-based mobility restrictions. Evidence from a 2023 CGAP study[8] shows that women customers are more likely to engage with and seek advice from female agents, who play a crucial role in building confidence and increasing women's use of DFS.

By leveraging automation and digitalisation, DFS significantly reduce the cost of customer acquisition, loan origination and transaction processing. Unlike traditional financial products and services, DFS can offer small-value loans and services sustainably, making them ideal for SMBs. DFS also enable real-time fund transfers, allowing businesses to respond quickly to inventory needs, customer demand or emergencies. Leveraging the digital transaction history of an SMB – such as mobile money history, airtime usage or merchant e-wallet activity – DFS providers can generate alternative credit scores. These enable fast, data-driven loan decisions – often within minutes and even for customers without formal financial records.

DFS solutions enable women entrepreneurs to operate more efficiently and with greater autonomy. For example, in Sub-Saharan Africa, mobile money has seen rapid adoption, contributing to 55% of the global mobile money market with more than 283 million 30-day active accounts as of 2024,[9] enabling faster, more cost-effective financial access. Women entrepreneurs in Ghana use DFS almost as much as men, although they tend to use core services like person-to-person (P2P) transfers more frequently than non-core DFS like bill payments or savings.[10] In Kenya, women-led SMBs that accessed credit from fintech M-KOPA[11]

3 World Bank. (16 October 2019). Understanding Poverty/Topics: Small and Medium Enterprises (SMEs) Finance.
4 Dasaraju, H. and Tambunan, T.T. (2023). "Introduction: Role of MSMEs in Achieving SDGs: Perspectives from Emerging Economies". In: Dasaraju, H., Tambunan, T.T. (Eds.). Role of Micro, Small and Medium Enterprises in Achieving SDGs. Sustainable Development Goals Series.
5 Sivio Connect. (27 June 2025). "MSMEs are Africa's Backbone — Let's Strengthen Their Foundation!" Newsletter.
6 Women's World Banking. (2024). Advancing Women-Led MSMEs through Digital Financial Inclusion.
7 Muckerheide, M. (26 October 2023). "The finance gap for women entrepreneurs is $1.7 tr illion. Here's how to close it". World Economic Forum.
8 Hernandez, E. et al. (2023). Women Agents for Financial Inclusion: Exploring the Benefits, Constraints and Potential Solutions. CGAP Working Paper.
9 GSMA. (2025). The State of the Industry Report on Mobile Money 2025.
10 GSMA. (2022). Exploring women's use of mobile money in Ghana.
11 M-KOPA. (2025). M-KOPA Impact Report 2025: Pathways to progress.

to purchase smartphones reported a more than 50% increase in earnings, with 82% of smartphone users experiencing income growth.[12] Similarly, Tala[13] and Branch, microloan apps in Kenya, are frequently used by women for business purposes, such as to increase stock. In Bangladesh, the agent network of mobile money service bKash has successfully extended DFS to rural women entrepreneurs, allowing them to receive payments, pay suppliers and save digitally through local agents.[14]

Access to secure digital networks, DFS products and educational resources enables SMBs to grow more rapidly and operate safely in the digital economy. One of the key challenges facing SMBs in LMICs, especially in Sub-Saharan Africa, is low levels of formalisation, with the majority operating without trade licences, registered business names or formal bank accounts. According to the International Labour Organization (ILO),[15] more than 85% of employment in Africa is informal, and many SMBs operate outside regulatory and financial systems. This limits their access to credit, insurance and markets, as traditional financial institutions tend to favour formally registered businesses with verifiable transaction histories.

In response, many women entrepreneurs have turned to informal savings and credit groups, such as Village Savings and Loan Associations (VSLAs) as alternative sources of working capital. While these community-based models provide critical support and social trust, the funds that women can access are often insufficient to grow their business. Digital platforms, however, make payment flows more transparent and enable businesses to generate transactional records, improving their creditworthiness and eligibility for loans.

The Global Findex Database 2025[16] shows that digital payments are associated with increased business activity and transaction safety, with growing numbers of SMBs across Sub-Saharan Africa and Asia reporting greater business resilience as a direct result of adopting DFS. A study in Uganda shows that women entrepreneurs who received microfinance loans through digital accounts saw 15% higher profits and 11% more business capital compared to those without DFS loans.[17] Another study in Indonesia highlights that SMBs that have embraced digitalisation have increased their sales by 15%.[18] Therefore, secure digital channels not only protect revenue streams, but also expand opportunities for market integration and economic advancement.

The rise of DFS has also opened critical financial pathways for SMBs. According to Global Findex data, 75% of adults in LMIC economies now own a financial account and the gender gap has narrowed by five percentage points, with 73% of women owning an account. This surge in DFS – especially mobile money and digital payments – has significantly boosted financial inclusion. In Sub-Saharan Africa, about 40% of adults have a mobile money account, while in Latin America and the Caribbean, the figure is about 37%.[19] Digital payments have the potential to promote the economic empowerment and inclusion of SMBs, including those owned by women, by facilitating entry into the formal financial system, strengthening access to credit and other financial services and creating opportunities for greater income, productivity and investment of business earnings. Digital payments help to stabilise wages for many micro-entrepreneurs and self-employed women by decreasing the hidden costs of cash payments, making payments more reliable and offering a digital record for financial planning.[20]

Women-led SMBs that use digital payments are less likely to have erratic incomes because the payments make it easier to control cash flow and allow for more predictable income management.[21] Initiatives such as agent networks and fintech partnerships have enabled millions of women to access mobile payments, digital savings and flexible financing, narrowing gender gaps in financial engagement. The transformation is evident in case studies from Kenya, Ghana and Bangladesh, among other countries. In Kenya, for instance, the Lipa Na M-PESA[22] service has grown from 170,000[23] merchants in 2020 to 700,000 in 2025.[24] The service has allowed many women micro-retailers to accept digital payments, reducing theft risks and providing transaction histories that improve access to working capital loans.

12 Holmes, T. and Maylie, D. (11 June 2024). "Thanks to My Smartphone, Business is Booming". IFC.
13 60 Decibels. (2022). Tala Kenya: Impact Performance Report.
14 BII. (2024). How can digital financial services drive women's economic empowerment in South Asia?
15 ILO. (30 April 2018). "More than 60 per cent of the world's employed population are in the informal economy".
16 Norris, A. and Singer, D. (17 July 2025). "Digital technology is unlocking financial inclusion". World Bank Blogs.
17 Riley, E. (2024). "Resisting Social Pressure in the Household Using Mobile Money: Experimental Evidence on Microenterprise Investment in Uganda". American Economic Review 114 (5): 1415–47.
18 Adjie, M.F.P. (11 January 2021). "Why today is the right time for Indonesian SMEs to go digital". Kata.ai.
19 World Bank. (2025). The Global Findex Database 2025.
20 Sirtane, S. and Singh, S. (15 July 2025). "Digital Payments Are Changing Women Entrepreneurs' Lives—What's Next?" CGAP.
21 De Gasperin, C., Rotondi, V. and Stanca, L. (2019). Mobile Money and the Labor Market: Evidence from Developing Countries. University of Milan Bicocca Department of Economics, Management and Statistics Working Paper No. 403.
22 Lipa Na M-PESA is a cashless payment service by Safaricom for businesses and individuals.
23 Safaricom. (9 November 2021). "Safaricom launches Lipa Na M-PESA business app".
24 HerBusiness. (2 August 2025). "How M-PESA transformed Kenya".

Country spotlight



DFS and women-led SMBs in Kenya

Kenya's digital financial revolution has demonstrated the transformative potential of DFS. Kenya offers a uniquely rich terrain for DFS research, having achieved some of the highest levels of mobile money penetration globally. Since the launch of the mobile money service M-PESA by Safaricom in 2007, Kenya has become a global leader in mobile money innovation. According to FinAccess 2024,[25] mobile money account ownership in Kenya is more than 82%, and access to formal financial services has grown from 26% in 2006 to 84% in 2024. DFS adoption has enabled millions to participate in formal financial activities, including credit, savings and insurance. This has significantly increased the number of banked individuals and enabled broader participation in the formal economy.[26] The small business sector has been a key beneficiary, leveraging mobile finance to improve operations, track payments, access new capital sources and grow customer bases.

Despite these gains, persistent barriers continue to limit equitable access for women. Social norms and patriarchal structures significantly influence women's privacy and security. While mobile phone ownership among women micro-entrepreneurs in Kenya is relatively high at about 80%,[27] phone sharing – although not common across the country – remains prevalent among lower-income or rural populations and is more widespread in other LMICs. In such contexts, shared phones can compromise privacy and security by allowing others, often family members, to access sensitive financial information or credentials.

Even for women with their own mobile device, low digital literacy can limit safe and independent use of DFS. Kenyan women, particularly those in rural or underserved areas, have lower digital literacy levels, limited access to smartphones and internet connectivity and heightened exposure to privacy and security threats.[28] Social norms and structural inequalities compound these challenges, often discouraging women from engaging with digital platforms or limiting their autonomy in financial decision-making. Addressing these disparities is essential to ensure that Kenya's DFS revolution benefits everyone.

Women-led SMBs in Kenya face distinct challenges in accessing and using DFS. The combination of business responsibilities, economic constraints and patriarchal norms amplifies privacy and security risks beyond those encountered by individual or male entrepreneurs.[29] Women entrepreneurs often juggle household responsibilities alongside business management, leading to time and cognitive overload. They may also face gatekeeping from male family members regarding financial decisions while being under greater scrutiny in their communities. These realities compound the challenges of accessing and using DFS safely.

More than other user segments, women-led SMBs in Kenya need services that support both personal and enterprise financial needs, as they often navigate personal and business matters from the same account or device. As such, privacy and security concerns are not just about technology – they are also about access, autonomy and empowerment. In many households, men may control finances and mobile phone use, sometimes monitoring women's activities. Women may feel compelled to disclose financial details to their male counterparts, which limits their privacy. This is compounded by lower levels of financial education, which can make women more exposed to pressure from men's requests.

25 Heyer, A., Makunda, L.J. and Juma, S. (6 May 2024). "The 2024 FinAccess Household Survey: Is Kenya's financial sector reaching its limits?" FSD Kenya Blog.
26 Misati, R. et al. (2022). "Does digital financial innovation enhance financial deepening and growth in Kenya?" International Journal of Emerging Markets, 19(3).
27 GSMA. (2024). Empowering women micro-entrepreneurs with mobile: Kenya findings.
28 *Ibid.*
29 Heyer, A. et al. (6 March 2025). "How digital technology is helping to close the gender gap in financial inclusion in Kenya". FSD Kenya Blog.

Privacy and security are essential to DFS, building user trust, protecting sensitive data and ensuring safe access – especially for underserved users like women-led SMBs. For these entrepreneurs, privacy and security are fundamental enablers of trust, participation and empowerment in the digital economy. When DFS providers clearly communicate how privacy mechanisms such as data collection, storage and protection are handled, women entrepreneurs are more inclined to use a range of DFS beyond basic money transfers, from digital savings and insurance to business loans and e-commerce platforms.[30,31] For women-led SMBs, secure DFS not only protect their financial assets, but also their personal dignity and autonomy.

Since DFS users entrust providers with highly sensitive personal and business data, providers often employ measures such as encryption, strict access controls and routine security audits to reduce risks of unauthorised access, fraud or misuse. Yet, when data breaches or unauthorised disclosures occur, they can result in severe financial and reputational damage, undermining both enterprise operations and customer confidence. For women-led SMBs, the stakes are even higher – privacy breaches can expose them to online harassment or financial abuse, eroding safety and making them more reluctant to use digital tools.[32]

Safe access to DFS is also shaped by authentication processes, fraud prevention tools and the reliability of transaction channels. Like other users, SMBs, especially in LMICs, often encounter cyber threats like phishing and scams that can lead to financial loss. Women-led SMBs may be at additional risk due to lower digital literacy, limited prior exposure to financial technology or fears about their personal security. To address these challenges, DFS providers are implementing accessible authentication options, integrating clear safety warnings and offering targeted user education. These measures help to mitigate risks and foster safer engagement with financial services. For example, the ITU's DFS Security Lab collaborates with regulators and providers to adopt international security standards, conduct mobile app security tests and deliver consumer competency frameworks aimed at improving digital literacy and safety.[33] By prioritising inclusion and actively safeguarding users' identities, service providers are enabling broader and more equitable financial participation.

Still, privacy and security gaps persist and can have serious, wide-ranging impacts. Even though DFS coverage has improved and usage is growing, many SMBs operate in markets where consumer protection regulations may not be well established and there can be an environment of opaque data-sharing practices, low levels of digital literacy and inadequate authentication systems.[34] Users may also have low awareness of online safety, particularly SMB owners. Wide-ranging repercussions include financial fraud, business interruption, sensitive data loss and loss of confidence in DFS providers, all of which diminish the inclusion benefits of DFS.

Poor privacy and security have a particular impact on women-led SMBs due to the persistent gender gap in DFS adoption,[35] the smaller scale of their businesses and resource constraints. Women entrepreneurs also often face systemic barriers that limit their access to digital tools and financial literacy programmes, making them more susceptible to privacy and security threats in the DFS ecosystem.[36] As a result, women-led businesses are less likely to benefit from emerging technologies or participate in digital upskilling initiatives.[37] This further limits their ability to adopt secure and efficient financial solutions.

Limited access to capital and smaller operational footprints also mean that DFS providers often grapple with financing the infrastructure or support systems needed to implement robust cybersecurity measures.[38] Studies show that women-led SMBs are disproportionately affected by data breaches, fraud and service disruptions,[39] which further entrenches inequality and hinders their ability to grow and compete in the digital economy.

Perceptions of privacy and security among women-led SMBs are shaped by both individual experiences and broader cultural contexts in which privacy becomes a matter of dignity, independence and protection from social scrutiny or exploitation. While structural gaps are evident, women-led SMBs interpret and respond to privacy and security risks in deeply personal ways. Their perceptions are informed by experiences of surveillance, informal power dynamics and gendered scrutiny in both household and business contexts. For many, digital privacy equates to autonomy and safety, safeguarding not just data but also social standing and independent decision-making. In patriarchal settings, breaches

30 GSMA. (9 September 2024). "Limited usage: women and mobile money in Tanzania".
31 GPFI. (2020). Global Partnerships for Finance: Advancing women's digital financial inclusion.
32 World Bank. (n.d.). "Digital financial inclusion barriers: Demand-Side Barriers".
33 ITU Initiatives: Digital Financial Security Lab.
34 Chalwe-Mulenga, M., Duflos, E. and Coetzee, G. (2022). The Evolution of the Nature and Scale of DFS Consumer Risks: A Review of Evidence. CGAP.
35 GSMA. (2025). State of the Industry Report on Mobile Money 2025.
36 Khera, P. et al. (December 2022). The Digital Gender Gap. International Monetary Fund (IMF).
37 Women's World Banking. (2024). Advancing Women-Led MSMEs through Digital Financial Inclusion.
38 Cyber Readiness Institute. (30 April 2024). "Small and Medium-Sized Businesses Face Major Obstacles in Achieving Cyber Readiness: The State of SMB Cyber Readiness, 2024". Press release.
39 AFI. (2023). A Policy Framework for Women-Led MSME Access to Finance.

in financial privacy may carry reputational or interpersonal consequences far beyond the loss of income or data. These lived experiences underscore the need for DFS to address both technical vulnerabilities and social risks.

The lived experience of women-led SMBs, including the need to navigate restrictive gender norms and heightened exposure to fraud or surveillance, demand privacy and security measures that are not only robust but also responsive to their unique realities.

An inclusive DFS architecture must recognise that risks are not felt equally. For women-led SMBs, every transaction or digital interaction may intersect with cultural expectations, economic precarity and gender-based constraints. The need for secure, private and user-friendly DFS solutions is not only a technical requirement but a matter of enabling equitable access and safeguarding livelihoods. Solutions must be localised, participatory and sensitive to social norms, reflecting the actual needs and priorities of women entrepreneurs operating at the margins of formal finance.

Scope and research objectives

This white paper examines the perceptions, expectations and experiences of women-led SMBs navigating privacy and security risks across the DFS ecosystem. It draws on insights and findings from research in Kenya to generate lessons for other emerging markets. It aims to:

- Explore how women-led SMBs perceive and experience privacy and security with DFS
- Identify the systemic and contextual factors shaping these experiences
- Inform the design of DFS that are inclusive, user-centric and attuned to gender-specific risks

Target audience

The primary audience for this white paper includes DFS providers such as fintechs, mobile money providers and digital banks, particularly those focused on small business segments in Kenya and comparable markets. These providers are well positioned to design, adapt and deliver services that address privacy and security expectations from the ground up. A secondary audience is development partners and ecosystem enablers, such as the GSMA and Visa, which can support research, innovation and capacity building to ensure DFS systems work for all users, especially women-led SMBs.

Methodology

The study employs a mixed-methods research strategy, combining a comprehensive review of secondary literature with primary qualitative data collection from key informant interviews (KIIs) across the DFS ecosystem. Primary data was collected in 18 KIIs conducted between February and May 2025 with a range of stakeholders who provided insights on the privacy and security of women-led SMBs that are using mobile to access DFS. The stakeholders included banking institutions, fintechs, microfinance institutions (MFIs), development organisations, digital technology companies, mobile network operators (MNOs), consumer organisations and regulators.

The qualitative methodology focused on uncovering gendered experiences, with Kenya serving as a proxy for broader trends in emerging market engagement with DFS products. The study also integrates insights from the Visa Consumer Empowerment Study conducted between 2022 and 2024, which surveyed 39,100 adults globally across 30 markets, including 1,200 respondents in Kenya, to understand consumer behaviour around data collection and sharing, and to identify key factors that influence consumer trust.

2. Perceptions and expectations of DFS privacy and security

DFS have become indispensable tools for women-led SMBs, particularly in LMICs like Kenya where mobile money and other DFS are central to daily business operations. However, the decision to engage with DFS is not purely functional. It is deeply influenced by how women perceive and trust the system to protect their personal and business data.

Privacy and security are fundamentally important in the context of DFS because financial services are inherently based on trust. Inadequate privacy and security expose users to fraud, scams and financial theft. Scammers can steal identities and use them to register on different DFS platforms, creating debts for victims. Multiple informants highlighted that women, particularly in rural areas, are at greater risk than men to privacy and security infringements. They are often seen as more susceptible to fraudulent schemes since a lack of awareness and tendency to be more trusting can make them prone to being duped.

Conversely, strong privacy and security measures foster confidence and trust in the system, which lead directly to increased adoption and ongoing use of DFS. For women-led SMBs, feeling assured of security and privacy increases usage and allows them to explore more financial services. This builds confidence, trust and a willingness to refer products to other women, ultimately expanding the reach of financial services. This confidence also allows them to grow their businesses, save and transact more and access other markets – all pathways to greater economic stability and financial health.

Perceptions of privacy and security when accessing DFS

Perceptions of privacy and security are critically important when it comes to using mobile to access DFS because decisions to use DFS are shaped by how secure a user feels, how informed they are and how transparent the service provider appears. For women-led SMBs, these perceptions directly influence adoption, usage and trust – all of which are essential for digital inclusion and economic empowerment. They affect whether women-led SMBs will open a digital account, opt for a digital loan or transition from cash to digital payments. These attitudes are foundational – not only for uptake, but also for how DFS can catalyse broader economic empowerment, support business growth and enhance women's autonomy in financial decision-making.

Perceptions of privacy and security are particularly important in the early stages of adoption and use because they are often formed before a woman has fully adopted a financial service. They are shaped by social networks, media reports and prior experiences with DFS. Importantly, they act as psychological filters that determine whether a woman feels safe enough to even begin using DFS. In this sense, perception is not just a consequence of experience – it can also be a barrier to or enabler of engagement.

For DFS providers, perceptions of privacy and security make the onboarding experience and initial user interactions critical. If the onboarding process is opaque, consent terms are hidden in legalese or peers share stories of data misuse, many women will opt out before any financial value is realised. As the Visa Consumer Empowerment Study for Kenya (2024)[40] shows, only 11% of Kenyan consumers fully understand how their data is being used and 64% report that companies only sometimes, rarely or never educate them about data usage and controls. Without clarity and trust at this early stage, adoption stalls, particularly among women who are already socially or financially marginalised.

Women entrepreneurs often view DFS with caution due to concerns about fraud, unauthorised data use and exposure of sensitive personal or business information to partners or communities. Key perceptions include the vulnerability of DFS platforms to hacking and fraud, weak or cumbersome authentication processes, lack of user-friendly explanations about security features and vague or one-sided privacy policies that emphasise provider protection over user empowerment. Beyond data and technology concerns, social scrutiny is a significant fear: women worry that larger or frequent transactions could provoke suspicion, jealousy or even backlash from spouses or extended families, jeopardising their autonomy and dignity. This aligns

40 Visa. (2024). How Empowering Consumers Promotes a Trusted Digital Economy. Visa Consumer Empowerment Study for Kenya. Unpublished report.

with the consumer scepticism observed in Visa's studies, where a majority believe financial institutions collect excessive personal data and leverage it more for their benefit than consumers.

The KIIs and secondary data revealed five dominant perceptions among women-led SMBs:

1. **DFS are vulnerable to fraud and unauthorised access.** Many users believe that DFS platforms, especially mobile apps, can be compromised easily. In Kenya, women-led SMBs expressed specific concerns about unmasked SMS alerts or weak authentication measures. Some even cited experiences where family members accessed accounts without consent.
2. **Women lack effective control over their data.** Kenyan consumers reported limited awareness of opt-out mechanisms and often found consent processes unclear. According to Visa's Consumer Empowerment Study for Kenya (2024),[41] only 8% of consumers feel completely in control of how their data is being collected and used, and just 9% feel completely comfortable with how it is handled.
3. **Security features are not user-centred or sufficiently explained.** Interfaces often do not clearly explain security features, especially for non-tech savvy users. Informants indicated that many women-led SMBs would prefer biometric logins or clear icons signalling data encryption, yet these are rarely explained or emphasised. Moreover, while some women are aware of the existence of security features, many do not fully understand their own role in safeguarding against fraudulent activities. For example, they may not know how features like PIN confidentiality, two-factor authentication or regular password updates directly affect their personal and business security, which leaves them at risk, even when protective tools are available.
4. **DFS providers prioritise their own interests.** A common perception is that data policies are designed to protect providers from liability, not to empower users. This creates a power imbalance whereby users feel compelled to accept terms they do not fully understand. Visa Kenya data also highlighted that 37% of consumers believe data use policies serve legal protection rather than user education.[42]
5. **DFS usage invites social scrutiny and potential backlash.** Informants highlighted that women are worried that using DFS for large or frequent transactions could draw suspicion or even backlash from partners or community members. Such suspicion often stems from fears of hidden income, diversion or misuse of funds or perceived involvement in outside relationships. In many cases, financial transparency within households can heighten tensions rather than build trust, particularly where traditional gender norms dictate who controls money. For many, privacy is not just about data but protecting one's autonomy and dignity.

These perceptions align with Visa's Consumer Empowerment Study findings, which showed that 85% of Kenyan consumers are concerned about unauthorised access to their data and 61% believe companies benefit more from their data than they do.[43] This scepticism shapes behaviour: many women entrepreneurs limit DFS use to low-risk transactions or revert to cash despite the known benefits of formal digital finance. Informants also highlighted that women-led SMBs often struggle to verify the legitimacy of alerts, protect their accounts and navigate complaint mechanisms effectively. One fintech informant explained, "You have dormant customers because they opted in, reviewed the terms, and decided not to continue – they were not confident their privacy would be protected." These actions are not passive disengagement but active self-protection strategies.

Expectations of privacy and security when accessing DFS

Expectations are shaped by perceptions. Once basic concerns about privacy and security are addressed, a user's expectations influence their continued use of DFS, satisfaction and loyalty. In the absence of experience, expectations are shaped by beliefs and cultural norms, information shared by others and community dynamics. Together, these beliefs form the foundation on which expectations are built. Women entrepreneurs often enter the DFS space with clear expectations about how providers should protect their data, safeguard transactions and provide transparency on costs and terms. These expectations, such as receiving timely fraud alerts, having control over data-sharing permissions or accessing responsive customer support, are critical guideposts for providers seeking to drive uptake and sustained use. While some expectations are informed by perceptions of digital finance (positive

41 Visa. (2024). How Empowering Consumers Promotes a Trusted Digital Economy. Visa Consumer Empowerment Study for Kenya. Unpublished report.
42 Ibid.
43 Ibid.

or negative), others stem from broader customer experiences or peer recommendations. Findings from Visa's Consumer Empowerment Study for Kenya show that more than 79% of consumers consider transparent communication about data use a decisive factor in continuing to share digital data.[44]

This underscores how important expectations are to customer retention. For providers, meeting expectations is not just about fulfilling a service promise – it determines whether women-led SMBs deepen their engagement with DFS, explore more advanced products like digital credit, savings or inventory tools or limit themselves to basic payments. Secure interfaces, clear communication and respectful onboarding are, therefore, central to building loyalty and advancing digital and financial inclusion.

Women-led SMBs have specific expectations of privacy and security due to their cautious perceptions of DFS and unique realities. These expectations are crucial for fostering continued use, satisfaction and loyalty in the digital financial ecosystem. The core expectations revolve around data protection and control, transparent communication and responsive redress mechanisms.

1. **Comprehensive data protection across all DFS types:** Women-led SMBs expect their personal and business data to be protected from misuse, unauthorised sharing, fraud and surveillance across all DFS platforms, including mobile money, digital banking apps, fintech credit platforms, e-wallets and agent networks. This expectation is driven by their perception that privacy is tied to dignity and self-worth. They anticipate strong authentication, confidential transaction processes and clear consent protocols for any digital financial activity. For instance, a key informant from the fintech sector highlighted the importance of features like "your voice, your password" to safeguard access to financial services for women in Kenya. This expectation is heightened for business-specific concerns, as women-led SMBs manage higher transaction volumes and maintain sensitive digital records (e.g. inventory). This necessitates robust security features and user-friendly interfaces to conceal business revenues from competitors or abusive partners.
2. **Transparency and user control over data usage:** Consumers want control over their data, but very few feel they have it. Women-led SMBs expect DFS providers to offer clear and transparent consent models, explaining data usage, opt-in/opt-out choices and available protections in accessible ways. According to Visa,[45] in the CEMEA region 57% of consumers want to know how their data will be used, while 50% want to know whether it will be sold or shared and 74% want at least the option for more control over their personal data. Additionally, half (50%) of consumers express strong interest in being able to easily change permissions when deciding to share data. This strong desire for transparency and control presents an opportunity for empowerment through more accessible and flexible data management options.
3. **Effective and accessible redress mechanisms:** When data breaches or abuses occur, women-led SMBs frequently lack access to timely, confidential and culturally sensitive dispute resolution options. They expect functional mechanisms that address their grievances, particularly given their heightened exposure to scams, unauthorised account takeovers and public disclosure of business transactions. Poor security often leads to incidents of violence and emotional distress. Key informants shared instances of women entrepreneurs experiencing self-doubt and lowered self-esteem when there is a breach in personal data, saying that "my husband transferred all the money to himself" due to lack of protection. Formal complaint processes are often intimidating or impractical, especially for those in rural settings or with limited literacy. Therefore, women expect accessible, community-level dispute resolution systems, like mediation forums or small claims courts, which are seen as more practical and trusted avenues for resolving DFS-related grievances.

44 Visa. (2024). How Empowering Consumers Promotes a Trusted Digital Economy. Visa Consumer Empowerment Study for Kenya. Unpublished report.
45 Visa. (2024). The Importance of Consumer Data Confidence. Visa CEMEA Consumer Empowerment. Unpublished report.



The gap between perceptions and expectations

The research indicated a noticeable mismatch between women's perceptions of privacy and security when accessing DFS and their expectations. While many women-led SMBs are unaware of specific privacy and security measures or their rights, they expect DFS providers will act responsibly and keep their information private, often overlooking their own role in managing it. This gap manifests in two ways: first, users expect security but encounter risk, and second, they seek control but find opacity. For many women-led SMBs, particularly in rural areas, the perceived risk of security is often greater than the actual risk. This perception is influenced by fears of fraud and harassment, even if these fears are not always realised. Some women view basic phone functions as insecure and express a clear need for digital safety training. Despite DFS providers often promising data protection, they fail to offer tangible tools, user-friendly controls or accessible redress pathways. As a result, this gap between expectation and reality undermines trust, limits uptake and disproportionately affects women's ability to benefit fully and safely from DFS.

There is also a mismatch between the perception that DFS are risky and unsafe and the expectation that DFS should be safe, transparent and user-friendly. When this gap is not addressed, women tend to restrict themselves to basic services like P2P transfers, avoiding more advanced offerings like digital loans or business analytics. As mistrust grows, valuable financial tools that could support growth are underused. The result is that women's economic potential is capped, as many avoid formalising or fully digitalising their businesses. At the same time, DFS providers miss out on building a loyal and expanding customer base due to shortcomings in product design and communication. According to Visa's Consumer Empowerment Study for Kenya, consumers are 24 percentage points more likely to trust a company that provides a granular consent experience compared to traditional Terms and Conditions (T&Cs).[46] This is a clear indicator that meeting expectations through user-centric design can shift perceptions and foster engagement.

Failure to close the gap between perceptions and expectations risks entrenching gender disparities in DFS access. Conversely, addressing it creates opportunities to expand market share, deepen engagement and contribute to broader financial inclusion goals. In Chapter 4, we highlight key considerations for DFS providers and ecosystem actors to respond to these challenges and move towards more inclusive, trust-based solutions.

46 Visa. (2024). How Empowering Consumers Promotes a Trusted Digital Economy: Visa Consumer Empowerment Study for Kenya. Unpublished report.

3. Privacy and security in a DFS ecosystem: key actors and solutions

A robust and inclusive DFS ecosystem depends on the coordinated actions of multiple actors, each with unique responsibilities for ensuring the privacy and security of users, especially for groups like women-led SMBs. This includes both public- and private-sector actors whose roles often intersect with policy, technology, service design and consumer engagement.

In a typical DFS ecosystem in LMICs, key actors include:

- Fintechs and other DFS providers, such as MNOs, digital lenders, platform-based marketplaces and payment aggregators
- Commercial banks and MFIs
- Regulatory authorities and central banks
- Consumer protection bodies, industry associations and civil society

While these actors may vary in form and scale across countries, they all play a role in establishing the trust, security and transparency necessary for women-led SMBs to adopt and benefit from DFS. In Kenya, for example, banks such as Equity Bank have implemented two-factor authentication and transaction alerts to enhance consumer protection in mobile and online banking. Tala, a leading digital lender, has introduced in-app security prompts and customer education modules to help users identify fraud risks through fraud awareness messaging. Meanwhile, Safaricom's M-PESA has long relied on PIN-based access and has more recently expanded fraud alert systems to curb SIM-swap and phishing threats. However, the coordination and comprehensiveness of privacy and security strategies often fall short of women's expectations.

Key sector actors and their role in privacy and security

1. **Fintechs and digital lenders:** These actors have embraced innovation in digital credit and often follow a mobile-first approach, expanding access to finance for individuals and small businesses that may lack collateral. Some providers collect rich datasets (e.g. SMS logs, phone usage, social media metadata) to determine creditworthiness and extend uncollateralised loans. While such approaches have improved the speed and reach of digital lending, they can also raise questions about transparency, data protection and user consent. Key informants described these platforms as useful, although potentially intrusive if appropriate safeguards are not in place. Some digital lenders require location and contact access, with limited explanation of how such data is stored or shared. Although providers like Branch, Tala and other fintechs in Kenya have introduced app-level security controls, many women remain unaware of how to revoke permissions or understand the factors influencing loan decisions.
2. **MNOs:** MNOs are critical infrastructure providers, facilitating mobile wallets and data flows across DFS platforms. Their control of KYC data during SIM registration, along with their access to transactional data, gives them a powerful role in ensuring secure and responsible usage. However, SIM swap fraud and unauthorised access via shared phones remain persistent concerns in LMICs. In Kenya, Safaricom introduced voice biometric SIM registration to support KYC authentication processes and curb identity fraud when providing customer service support. This eliminates the need for vetting or securing questions to verify ownership. It also makes it possible for customers, including the visually impaired, to speak a simple voice pass phrase for authentication, and enables customers to access more self-service options easily and quickly. Beyond infrastructure and fraud prevention, MNOs also have a responsibility to provide customer education and ongoing user support, particularly for women who may face greater challenges in understanding or applying digital safety measures. This can be achieved through simple, step-by-step customer value management (CVM) messages, as well as through visual and accessible materials such as posters, brochures and radio campaigns that clearly explain how to identify scams, safeguard SIMs and report suspicious activity. Education efforts such as these strengthen user confidence and enhance the overall security of the DFS ecosystem.

3. **Commercial banks and MFIs:** Traditionally trusted for savings and credit, banks and MFIs increasingly offer digital channels (apps, USSD) that target micro-entrepreneurs. While their reputation lends trust, their digital platforms often lag fintechs in usability and transparency. In Kenya, Equity Bank's EazzyBanking app introduced biometric login and in-app fraud alerts, which respondents in our study viewed positively. At the same time, simplifying terms of service and consent processes presents an opportunity to strengthen user trust and inclusion, particularly for low-literacy populations.
4. **Payment aggregators and marketplaces:** Actors like Pesapal and Jumia Pay handle transaction routing and increasingly collect behavioural and preference data. Yet, few payment aggregators and marketplaces articulate their privacy policies in local languages or simplified formats. This fuels suspicion, especially among women who rely on these platforms for business-to-business (B2B) or business-to-consumer (B2C) transactions.
5. **NGOs, civil society and consumer organisations:** These organisations play a vital role as grassroots connectors with strong credibility among underserved communities. They have capacity for direct outreach, targeted education and advocacy for inclusive policy reforms. A banking regulatory informant in Kenya highlighted the ability of community-based NGOs to "reach rural and marginalised communities in smaller niche segments". Development partners also contribute significantly by delivering technical assistance and capacity building through digital and financial literacy programmes designed specifically for women nano-entrepreneurs.[47] Consumer organisations are crucial in advocating for and educating women consumers to "know their rights and detect privacy infringements". These civil society actors are pivotal in embedding gender-sensitive frameworks and amplifying women's voices to influence protective legislation and service design.
6. **Regulators and government entities:** Public regulators, such as central banks, data protection authorities, communications authorities, credit information sharing and consumer protection agencies, set the legal parameters within which DFS actors operate. For example, in Kenya, the Office of the Data Protection Commissioner (ODPC) plays a central role in enforcing the Data Protection Act of 2019,[48] including requirements around user consent and data breach disclosure. The Communications Authority of Kenya (CAK) also regulates aspects of mobile and internet service provision that directly affect DFS operations. However, enforcement efforts are still evolving, and many women-led SMBs are unaware of their rights under such legislation.

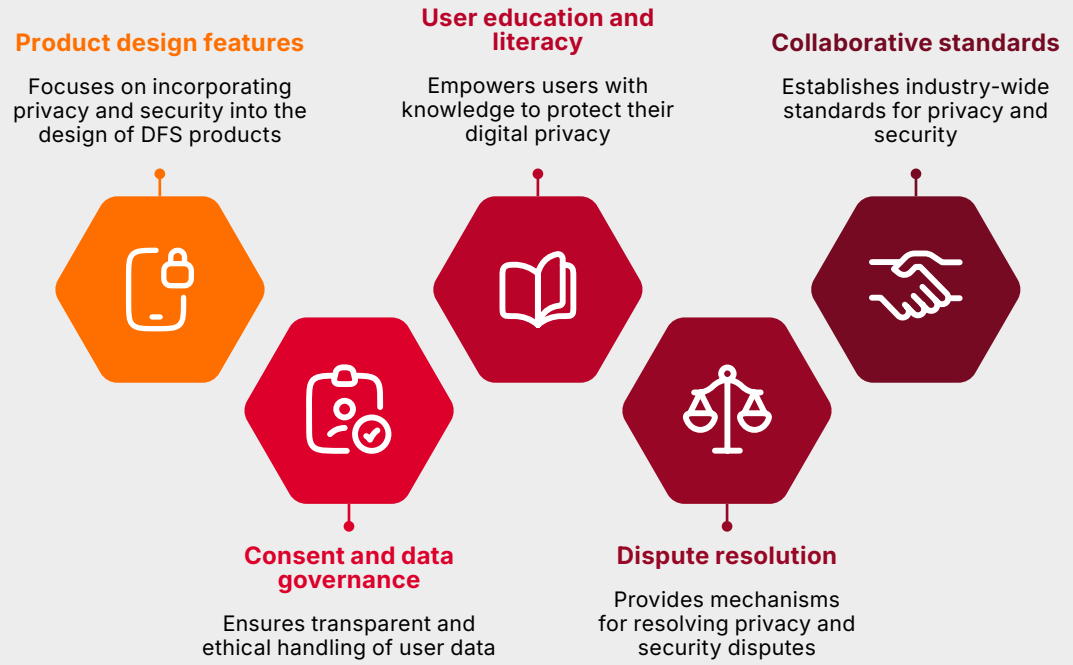


47 GSMA. (2025). Advancing Digital Financial Literacy: Insights from two pilot projects In Africa.
48 ODPC. (2019). Data Protection Act, 2019.

A taxonomy of privacy and security solutions for DFS

DFS providers across the ecosystem implement various types of privacy and security solutions, often in response to regulatory pressure or rising user expectations. Based on our research, these can be categorised into five types of solutions:

Figure 1:
A taxonomy of privacy and security solutions in the DFS ecosystem reveals five primary intervention types



Each type of solution offers distinct benefits and addresses different aspects of women's privacy and security concerns. Yet, our analysis found critical gaps between user expectations and the effectiveness of current solutions.

Product design features:
securing access, interfaces and communication channels

Design solutions include secure login (e.g. PIN, biometrics, multi-factor authentication or MFA), balance masking, SMS obfuscation and app-based privacy settings. In Kenya, one MNO improved adoption after removing phone numbers from mobile statements: "Women felt safer once names and numbers were hidden," a key informant noted.

Gap: These features are often inconsistently implemented and rarely customisable. Shared phone use remains a challenge and design decisions are typically made without user testing with women-led SMBs.

Consent and data governance protocols:
managing the collection, use and sharing of data

Strong governance includes granular consent prompts, opt-in data sharing and transparent terms of service. Visa's 2024 CEMEA study found that 62% of users are more likely to share data when companies explain its use simply and clearly.[49]

Gap: Most platforms default to complex legalistic terms, overwhelming women users with low literacy. In Kenya, only 8% of consumers felt fully in control of their data, revealing a significant power imbalance in consent.

User education and digital literacy:
empowering users to understand and manage risks

Education efforts delivered via SMS, in-person or community radio help women identify phishing, understand privacy settings and know their rights. Grassroots training by NGOs has proven effective, particularly for rural merchants.

Gap: Education remains siloed, underfunded and disconnected from product features. Women often rely on peers or agents for support, who may be poorly trained themselves.

Dispute resolution mechanisms:
providing accessible recourse when harm occurs

Robust redress systems, such as call centres, in-app reports and ombudsman services are critical for restoring trust after data breaches. Some Kenyan fintechs now offer chat-based support while community-based forums show promise for local justice.

Gap: Formal redress remains intimidating or inaccessible, especially for women in rural areas or with low literacy levels. Many do not report breaches due to shame, fear or lack of time. A key informant said, "Even if I complain, will they help me?"

Collaborative standards and industry governance:
aligning ecosystem-wide practices

Cross-sector coalitions, such as industry associations, gender working groups and regulatory sandboxes, can harmonise standards and reduce fragmentation. Kenya's nascent Data Protection Taskforce and Financial Sector Deepening (FSD) programmes offer promising models.

Gap: Competitive dynamics limit collaboration and only a few forums include direct representation from women-led SMBs. As a fintech informant noted, "We need to stop working in siloes – privacy is everyone's problem."

Despite progress, significant gaps persist between the expectations of women-led SMBs and the realities of privacy and security practices in DFS. Across product design, data governance, literacy, redress and standards, solutions are often non-inclusive, inconsistently applied or insufficiently user-centric. Such gaps erode trust, limit DFS adoption and constrain the economic potential of women-led SMBs. As Chapter 4 will explore, closing these gaps requires a set of practical considerations that centre women's lived realities, align ecosystem actors and build a secure, inclusive digital financial future.

49 Visa. (2024). The Importance of Consumer Data Confidence: Visa CEMEA Consumer Empowerment. Unpublished report.

4. Women-led SMBs and DFS: privacy and security considerations

To unlock the full potential of DFS for women-led SMBs, providers must prioritise privacy and security features that build trust, enhance control and reflect women's lived realities. Women-led SMBs in LMICs are a vital economic segment, yet their ability to engage fully with DFS is hindered by privacy and security concerns. The findings from Kenya and the broader CEMEA[50] region reveal that these concerns often stem from a gap between women's perceptions and their expectations of DFS safety, transparency and usability.

This chapter outlines concrete considerations for DFS providers and development partners to address these gaps, strengthen trust and foster inclusive participation in the digital economy. These considerations are drawn from KIIs, ecosystem landscaping in Kenya and insights from consumer research, ensuring they reflect both lived experiences and broader industry perspectives.



Consideration 1: Design for privacy from the start

DFS providers should embed privacy and security principles at the design stage, using participatory approaches that include women-led SMBs in co-creation. Embedding privacy from the outset ensures that solutions address actual user needs rather than retrofitting security features in response to problems. Human-centred design (HCD) methodologies can help integrate women-led SMBs in product prototyping, field testing and feedback loops. This is particularly important in contexts where gender norms, literacy levels and device-sharing habits differ from those of the "default" user profile. For example, in Kenya, providers that engaged women entrepreneurs early in product development reported higher adoption and lower churn rates compared to those who implemented privacy changes after launch.[51]



Consideration 2: Simplify data practices and communicate clearly

Clear, transparent communication about data collection and use builds trust and empowers women users to make informed choices. Key informants cited "confusing" or "hidden" terms of service as a reason for many women-led SMBs' mistrust in DFS. Providers can improve clarity by using plain language, multilingual translations and visual aids such as icons or infographics. Short, layered privacy notices, delivered during onboarding and circulated periodically, can help reinforce understanding. Visa's Consumer Empowerment Study for CEMEA found that consumers are more likely to trust companies with a granular consent experience (55%) versus a traditional T&C experience (30%). Yet, many platforms continue to use dense, legalistic text that uses implicit, unclear and complex language.[52]



Consideration 3: Expand granular user controls

Women-led SMBs want more granular control over what data they share, when they share it and with whom. Granular controls give users agency, allowing them to selectively grant or revoke permissions for location data, contact lists or transaction histories. Without these controls, women often feel they must choose between full access or complete exclusion from DFS. In practice, this means many opt out of advanced features like digital credit or merchant analytics due to discomfort over data sharing. Providers could introduce dashboards where users can toggle permissions, receive alerts when data is accessed and set limits on data retention. For women entrepreneurs who rely on basic or feature phones, similar functionality could be delivered through simplified USSD-based options, such as prompts to confirm or deny data-sharing requests, or SMS alerts about data access. This ensures that privacy and security features are equitable and accessible across device types, bridging the digital divide and enabling broader participation in DFS.

50 The Importance of Consumer Data Confidence: Visa CEMEA Consumer Empowerment. Unpublished report.
51 IFC. (2024). Her Fintech Edge: Market Insights for Inclusive Growth.
52 Visa. (2024). The Importance of Consumer Data Confidence. Visa CEMEA Consumer Empowerment. Unpublished report.

Consideration 4: Strengthen discreet access and transactional privacy

Enabling discreet access to DFS is critical for women navigating social norms, shared devices or familial scrutiny. In some communities, visibility into a woman's transactions can lead to social pressure, demands for financial support or even conflict. DFS providers can address this by offering features such as "private mode" logins, the option to hide balances on-screen and the ability to disable or mask SMS notifications. Alias-based payments where the recipient sees only a username, not a phone number can also protect user identity. Mobile tokenisation offers a powerful way to enhance privacy and security for all users, especially women seeking greater control over their personal information.[53] These discreet use features are rare in DFS ecosystems in LMICs, but could have outsized impact for women entrepreneurs managing sensitive business and household finances.

Consideration 5: Build robust and gender-sensitive recourse mechanisms

When privacy or security incidents occur, women-led SMBs need fast, respectful and accessible pathways to seek redress. Current recourse systems often lack transparency, speed or empathy. Some women in our Kenya study reported being blamed for fraud or data breaches, which discouraged them from reporting future issues. DFS providers can improve their privacy and security frameworks by:

- Training customer support agents in gender sensitivity and digital rights
- Offering multiple complaint channels (e.g. phone, in-app chat, community agents)
- Providing clear timelines for resolution and follow-up updates
- Involving trusted intermediaries in the recourse process, such as women's business associations, can increase trust and uptake

Consideration 6: Partner with development actors to scale inclusive solutions

Collaboration with development partners can help DFS providers pilot, refine and scale privacy and security solutions that centre women's needs. Development organisations, NGOs and donor agencies can offer technical assistance, fund pilot programmes and facilitate learning between markets. For instance, Visa and the GSMA partnered with two mobile money providers in Sub-Saharan Africa and in 2024 signed a pilot with Safaricom to deploy digital financial literacy content and training for mobile users in Kenya.[54] As part of this initiative, 12 million M-PESA app users now have access to digital financial literacy content. This was an industry-led effort to deliver locally relevant training that can improve feature adoption and awareness of data practices among women users. Partnerships can also enable joint research to monitor the effectiveness of privacy and security features, ensuring that solutions evolve alongside user needs.

Consideration 7: Establish metrics to track privacy and security

Without clear and consistent metrics, it is difficult to know whether privacy and security measures are genuinely empowering women-led SMBs or are simply "tick-box" features. DFS providers, regulators and development partners should embed monitoring and evaluation (M&E) frameworks that capture not just adoption, but also effective use, confidence and perceived safety among women users. These frameworks should include recourse indicators, such as the volume of complaints related to privacy or security, resolution timelines and levels of user satisfaction. Moreover, usage indicators, including the number and frequency of women actively engaging with privacy-enhancing features like consent settings, authentication tools or fraud alerts, could also be tracked. At the ecosystem level, aggregated reporting on these indicators can help identify systemic weaknesses, reveal gaps in user understanding and guide investment in targeted digital literacy and product improvement efforts. By institutionalising such metrics, DFS ecosystem actors can ensure that privacy and security interventions are not only technically robust, but also socially effective, strengthening women's trust and sustained engagement in the ecosystem.

53 GSMA Inclusive Tech Lab. Digital Safety for Gender Inclusion website.
54 *Ibid.*

5. Conclusion

Addressing privacy and security is not only a matter of compliance – it is also a pathway to more inclusive, trusted and impactful digital financial systems. For women-led SMBs, the ability to engage confidently in the digital economy hinges on whether DFS providers can meet their privacy and security expectations. By integrating user-centred design, simplifying data practices, expanding control, enabling discretion, strengthening recourse and partnering for scale, DFS providers can bridge the trust gap identified in this white paper. Doing so will not only empower women entrepreneurs but also unlock untapped market potential in LMICs.



GSMA Head Office
1 Angel Lane
London
EC4R 3AB
United Kingdom
gsma.com

GSMA
Mobile for Development

M4D