Building Financial Resilience Against Digital Risk

Strive Women Insights on Cybersecurity from the Midline Survey

July 2026

For a woman running a micro or small business (WMSE), going digital is a necessary growth strategy. A mobile wallet lets her conduct and track high volumes of transactions. Social media reaches customers she could never have served from her storefront. Digital access to her bank account provides her a safe place to store her money.

But the same digital activity that drives growth also expands the opportunity for fraud or consumer protection risk. Every new channel is another way for a scam to reach her.

> **"When I started using WhatsApp and all that, I was very afraid [of scams] … But I dared to do it. I had to take the risk."**
>
> — Entrepreneur, Peru

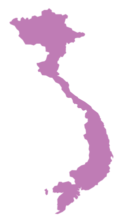
Strive Women, a four-year program led by CARE, is part of Mastercard Strive, a portfolio of philanthropic small business programs supported by the Mastercard Center for Inclusive Growth. It focuses on growth-oriented entrepreneurs who have been in business for at least two years and have at least one employee. While there is variation among participants, the typical entrepreneur is a married woman in her late 30s to early 40s with a secondary school education. Her business is most often urban-based, unregistered, and operates in the retail sector.

The findings in this learning brief draw on the Strive Women Midline Survey, conducted by 60 Decibels, which measured how women micro and small enterprise owners across Pakistan, Vietnam, and Peru experience and respond to digital financial risk and fraud. The sample composition is as follows:

Sample composition of Strive Women Midline

Pakistan
530 Respondents
459 Female **71** Male

Peru
368 Respondents
365 Female **3** Male



Vietnam
218 Respondents
193 Female **25** Male

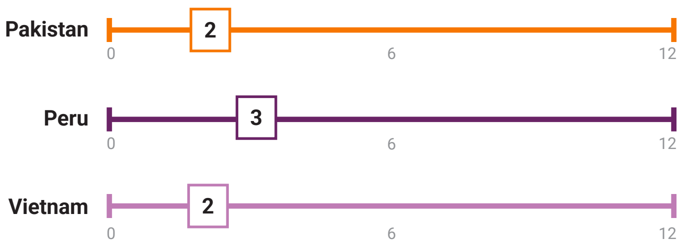
Due to the limited male sample, results in this brief focus on insights from female respondents only.

Digital tools are important for business growth, but tool usage increases exposure to risk.

The Strive Women midline survey reveals that sampled WMSEs place a growing importance on the use of digital tools for business growth. The data shows that 83% of Pakistani respondents, 81% of Vietnamese respondents, and 92% of Peruvian respondents use at least one digital tool. Moreover, on average, women use more than one tool, the most common tools being mobile wallets, online platforms for selling, and social media.

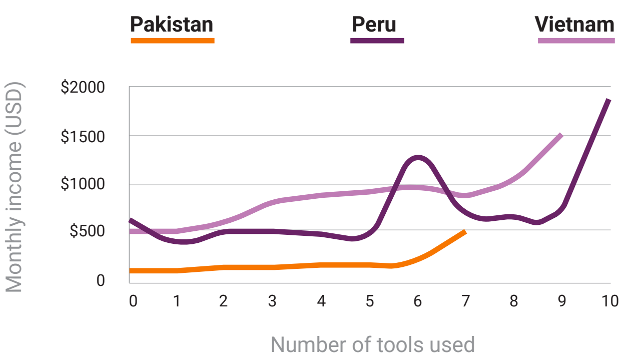
Number of Digital Tools Used

On average, entrepreneurs use multiple digital tools to run their business



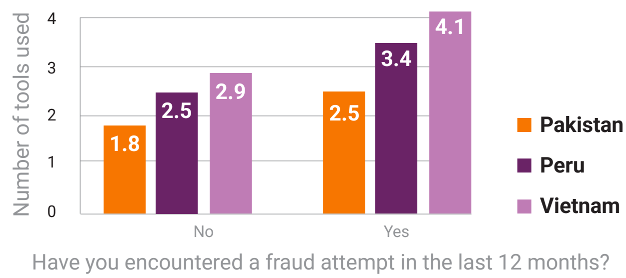
The data also shows that across all three markets the number of tools a woman uses is positively correlated with an increase in monthly business profit, suggesting going digital is a key driver of business growth.

Monthly income is positively correlated with number of digital tools used



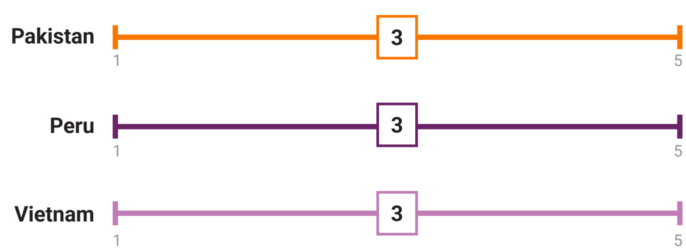
However, that same growth comes at a cost. Exposure to scams, fraud, and cybersecurity risks rises with use: women respondents in Vietnam and Peru – the higher-adoption markets – encounter digital scams at roughly twice the Pakistani respondents (21% Vietnam, 19% Peru, 12% Pakistan). The graph below demonstrates the average number of digital tools used by individuals who have experienced scams versus those who have not.

Potential fraud exposure increases with the number of digital tools used



While women's participation in the digital ecosystem is increasing, research from Accion shows that a "security divide" threatens these gains (Zukaneni et al. 2026). The same study found that women are 26% more likely to be approached by financial scammers, and 62% of women who avoid digital financial services cite security and fraud fears as reasons for non-adoption.

On a scale of 1-5, entrepreneurs say they are ‘not sure’ if digital platforms can adequately protect their data



> **“Customers would send screenshots claiming they had made the payment, but the money never actually reached my account. They would edit those screenshots to trick me.”**
>
> — Iraj, Pakistan

Digital participation opens new economic opportunities for WMSEs, but it also exposes women to risks such as frauds, scams, and financial loss. As such, epanding access alone is not enough. Supporting women's digital journeys also requires strengthening their ability to prevent, withstand, and recover from digital shocks, which can deplete savings or working capital in an instant.

A fraud event functions much like any other economic shock, capable of draining savings or working capital in a single moment. Within its Financial Health Framework, CARE defines financial resilience as the “ability of women entrepreneurs to **1) prepare for, 2) withstand, and 3) recover from shocks**.” In the context of digital risks, data from the Strive Women midline survey reveals gaps at each of these three stages.

Building Financial Resilience
in the context of digital risk, cybersecurity, and online fraud

Preparing for shocks	Withstanding shocks	Recovering from shocks
Protective habits that reduce the chance of a fraud or security event such as strong passwords, two-factor authentication, antivirus, backups, staff education.	Knowing what to do when something goes wrong: recovery steps, who to contact, what redress and institutional options exist.	The financial buffer available when a shock becomes a monetary loss; her capital reserves and emergency financing options.

I. Preparing for shocks

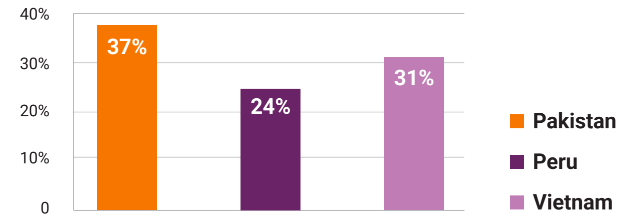
The midline data demonstrates that WMSEs recognize that taking actions to protect their business against digital risk is important for their business: 64% of Pakistani respondents, 83% of Vietnamese respondents, and 85% of Peruvian respondents consider cybersecurity important for business sustainability. This suggests that, within this segment, the barrier is not a lack of awareness but a failure to translate that awareness into action.

On a scale of 1-5, WMSEs rate the importance of cybersecurity as a “4” for their business.

However, preparing for digital shocks requires more than recognizing the risks. It requires taking concrete steps before something goes wrong. Findings from the Midline Survey suggest that awareness does not always translate into action. 37% of respondents from Pakistan, 31% in Vietnam, and 24% in Peru reported taking no steps to protect their businesses against digital risks. This gap may reflect uncertainty about what actions to take rather than a lack of motivation. While many respondents recognize the importance of cybersecurity, the specific practices and tools needed to protect their businesses may be less clear.

Indeed, when women do protect themselves, the majority indicate that the only step they take is setting and maintaining strong passwords for online accounts. Few other protective actions are taken beyond that one habit – and this is consistent across all markets.

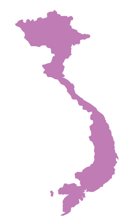
1 in 3 WMSEs do not take any steps to protect their business from digital threats



Which of the following actions do you take to protect your business from online threats?

> **"Many times I get messages or calls from strangers that are like scams, but I have been cautious. I have to be careful."**
>
> — Ha, Vietnam

Protective Actions Taken by Women Entrepreneurs

Pakistan 	**Peru** 	**Vietnam** 
60% Creating and managing strong passwords	**66%** Creating and managing strong passwords	**62%** Creating and managing strong passwords
22% Two-factor authentication	**12%** Two-factor authentication	**43%** Two-factor authentication
16% Backing up business data	**32%** Backing up business data	**35%** Backing up business data
11% Using antivirus software	**28%** Using antivirus software	**26%** Using antivirus software
6% Training staff on cybersecurity	**7%** Training staff on cybersecurity	**28%** Training staff on cybersecurity

Qualitative evidence from the midline survey shows that training and education on digital safeguarding, alongside the use of digital tools can increase WMSE's ability to prepare for shocks. One entrepreneur from Pakistan says, *"Before the [Strive Women] training, I was very scared to take risks, and I was even scared of the scams. But during the training, they guided us on how to take action during any kind of digital scams or fraud. So, I am now very much aware of everything."*

A 2023 survey conducted by WeConnect supports this finding: 84% of respondents from WMSEs outside the United States indicated that they needed more tools and training to improve their business' cybersecurity (WeConnect 2023).

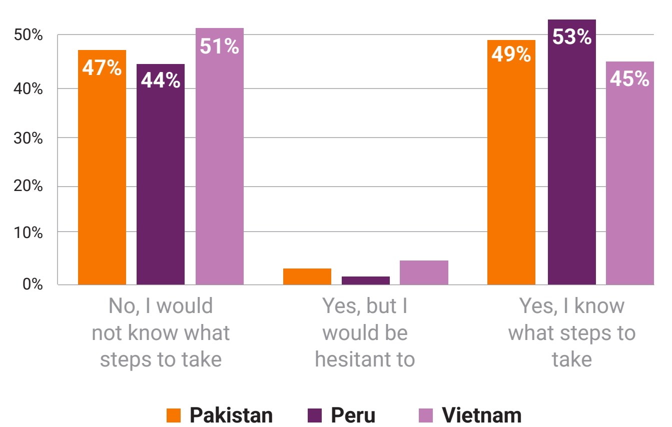
II. Withstanding shocks

> **"There was money taken from my card. I went to the bank. They told me I had made that withdrawal — but I had not."**
>
> — Entrepreneur, Peru

An entrepreneur's ability to withstand a shock means knowing how to respond in the moment: what steps to take, who to contact, and what redress options exist. Here, the findings from the midline survey reveals a gap between confidence and capability: despite high levels of comfort using digital tools, responding entrepreneurs are split on what to do when something goes wrong. About half of surveyed WMSEs would not know what steps to take if they realized their online account had been compromised.

On a scale of 1-5, WMSEs report high levels of confidence using digital tools.

Yet, 1 in 2 WMSEs would not know how to recover their digital financial account if there was an access issue.



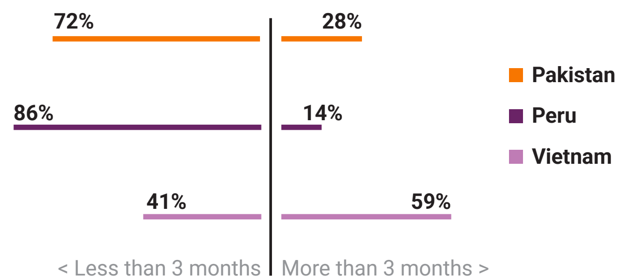
This, coupled with WMSEs' ambivalence about trusting digital service providers (demonstrated earlier), suggests that if a fraud event does occur, many may not know about, or trust, the redress options available to them, whether inside the bank or through external channels like government consumer protection programs.

III. Recovering from shocks

> **"In today's technology era, fraud is very common. Just one small mistake can cause the account to be completely wiped out."**
>
> — Entrepreneur, Vietnam

WMSE's ability to recover from a financial shock depends heavily on the capital reserves the business owner has access to. Results from the midline survey shows that when digital risk translates into a monetary loss, responding women are less likely to have the capital cushion needed to keep operating — and the thinner that buffer, the more harm a single fraud event can do.

70% of WMSEs, pooled across all three countries, would not be able to maintain their business for 3 or more months after a shock.



Respondents in Vietnam have the highest rates of resilience: 59% could cover three or more months of business expenses if there was a financial shock, meeting CARE's benchmark for whether or not a business is resilient. Respondents from Pakistan and Peru are far more exposed: only 28% of respondents in Pakistan and 14% of respondents in Peru could cover three or more months.

A significant portion of surveyed entrepreneurs have less than one month of reserves: 48% in Peru, 31% in Pakistan, and 23% in Vietnam. For anywhere from 1 in 5 to nearly 1 in 2 of these women, a single fraud event is not a setback to be absorbed, it is a significant threat to her business, her financial health, and livelihood.

Potential Solutions

When women's digital participation outpaces their ability to protect themselves from digital risks, both business growth and long-term sustainability are at stake. Building digital resilience requires support at every stage: helping women prepare by adopting protective habits, withstand incidents by providing clear recovery pathways and trusted avenues for redress, and recover with the savings and financial resources needed to keep the setback from becoming a business closure. No single actor can close these gaps alone; **the most durable solutions will combine what providers build into their systems, what programs teach and reinforce, and what regulators require.**

Security in design:
Private sector institutions, including mobile network operators, e-commerce platforms, and financial service providers, have a part to play here. Beyond formal training, online notifications, nudges, and messages placed throughout the user journey can build awareness of specific digital risks at different points of service. Institutions can also build default protections into products so that "safe use" does not depend only on women taking extra steps. This includes automatic multi-factor authentication, transaction alerts, safer onboarding flows for new users, and role-based permissions for business accounts to reduce internal fraud risk**.** (Zukaneni et al. 2026).

Trusted response and redress:
When a fraud event does occur, women need to know what to do and where to turn. Redress options should be made unmistakably clear, available, and no-cost across many channels: in-person support, online and in-app guidance, chatbots, and help-desks accessible by call or text. As the data gathered from the midline survey points to a trust gap as much as a knowledge gap, routing support through channels women already rely on matters. Trusted community structures like women's groups, cooperatives, and peer networks can serve as early-warning and reporting mechanisms and can offer a degree of anonymity that lowers the shame and stigma that often keep fraud victims silent or slow to report (Perlik et al. 2025).

Recovery and risk sharing:
Encouraging and enabling savings is among the most effective levers for recovery, since reserves are what separates a recoverable setback from a business closure (CARE 2025). Providers and programs can also explore fraud-loss protections and microinsurance built into online accounts, so that verified losses are partially absorbed by providers rather than solely by entrepreneurs.

Finally, and perhaps most critically, **protection should be discussed alongside business growth, not as a separate or secondary conversation.** And, when digital adoption is promoted, the means to use it safely should be promoted with it.

About Strive Women

Strive Women, a four-year program led by CARE, is part of Mastercard Strive, a portfolio of philanthropic small business programs supported by the Mastercard Center for Inclusive Growth. Through a Women-centered Design (WCD) approach, it strengthens the financial health of women-led small businesses in Pakistan, Peru, and Vietnam by delivering tailored 1) financial products, and 2) support services, such as digital skills building and mentorship programs. To date, Strive Women has delivered more than $500M in credit capital to entrepreneurs through local financial service providers (FSP) partners.

Want to partner with us?

entrepreneurship@care.org
www.care.org/entrepreneurship