

Building Critical Capabilities to Combat Digital Financial Fraud

Evidence from a randomized trial with 27,162 mobile money users in Uganda

Matthew D. Bird (Universidad del Pacifico) and Rafael Mazer (Fair Finance Consulting) • May 2026

In partnership with Viamo, IPA Uganda, and the IPA Consumer Protection Research Initiative, generously funded by the Gates Foundation.

KEY MESSAGE

We tested a phone-based fraud-prevention game with 27,162 Ugandan mobile money users. Users practiced spotting and responding to scams in a short interactive audio story, delivered free over any basic phone. Six to nine months later, trained users were **losing 20% less money to fraud**, saving more through mobile money, and filing **67% more fraud complaints** with the regulator. What made it work was **practice, not warnings**—the same SMS reminders we tested separately did nothing for untrained users.

The scam problem in digital finance

The expansion of telecoms and digital finance has opened new, fast-scaling ways for fraudsters to reach millions of potential victims at low cost. In 2024, mobile money processed **USD 1.68 trillion across more than 2 billion accounts globally (GSMA, 2025)**; the United States alone reported **USD 12.5 billion in consumer fraud losses (FTC, 2025)**. In East Africa, 61–86% of digital finance users say someone tried to scam them in the past year. Uganda sits in the middle of that range: **61% attempted, 9% victimized, USD 22 average loss (IPA, 2025)**.

Two standard responses are running out of road. Provider-side fraud detection is essential but reactive—fraudsters move faster than enforcement. Tip-and-warning campaigns, the dominant consumer-facing approach worldwide, raise general caution without reliably improving real-time judgment, and the effects fade within months (Kubilay et al., 2023; Byrne et al., 2024; Burke et al., 2022). What's missing is a **third approach**: teaching consumers a portable routine they can actually use in the moment.

The intervention: Beera Mubangule ("Be Ready")

The tool is a short audio game—an interactive voice story played by pressing keys on any basic phone. Users follow Sarah and Robert, a couple running a small business, through realistic scams: a call asking for a PIN, an impersonator claiming to be from the mobile money provider, a too-good-to-be-true prize. Users make choices under time pressure and hear what happens next. We made it available free on Airtel Uganda's *161 menu, working with Viamo and Innovations for Poverty Action (IPA Uganda and the IPA Consumer Protection Research Initiative). Three design principles drove the model:

1. PRACTICE, NOT TIPS Users practice handling scams in realistic simulations with feedback. They build a routine they can actually use, not just facts they can recite.	2. STOP–CHECK–ACT One portable action script: pause under pressure, verify through trusted channels, refuse/exit/report. Compact enough to recall, flexible across scam types.	3. SCALABLE BY DESIGN Audio over basic phones; works at any literacy level; marginal delivery costs near zero once zero-rated. Viamo already operates in 29 countries, 66 languages.
---	--	--

What we found

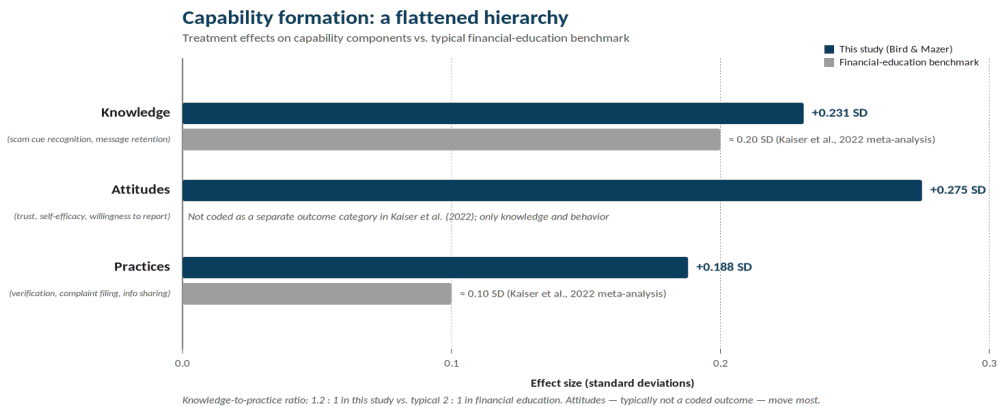


Figure 1. Capability decomposition. All three components moved strongly and survive multiple-testing corrections ($p < 0.001$). Typical financial education shifts what people know roughly twice as much as what they do; this intervention closed that gap.

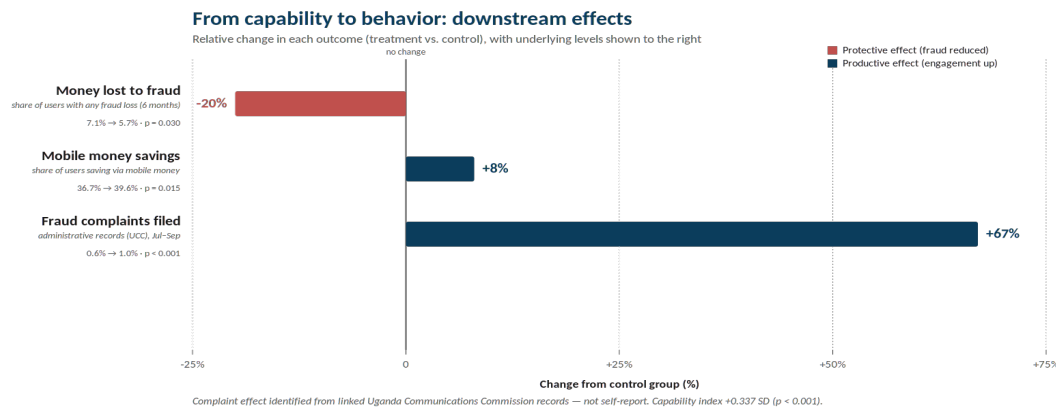


Figure 2. Downstream effects. Users who had recently been scammed used their new skills defensively (less money lost); users who hadn't been scammed used them productively (more savings, more reporting). Both groups engaged with mobile money more, not less.

1. Practice closes the knowing–doing gap. Typical financial education shifts what people know about twice as much as what they actually do (Kaiser et al., 2022). Our intervention moved attitudes and practices roughly as much as knowledge. The same SMS messages delivered to controls without training moved capability by only 0.026 SD (n.s.)—**information alone does not build capability**.

2. Reminders only work if people know what to do. We sent the same fraud-prevention SMS messages to two groups and tracked actual complaints to Uganda's regulator. Trained recipients turned the messages into action: fraud complaint filing rose (+0.36 pp from a 0.7% base, p<0.01). Untrained recipients did **nothing protective with the same messages**—if anything, their overall complaint filing was lower than pure control. Same information, opposite results. *Reminders activate skills people already have; they don't create skills people lack.*

3. Trained users engaged more with mobile money, not less. A common worry about fraud campaigns is that they scare cautious users away from formal financial services. We saw the opposite: trained users increased mobile money savings (+2.9 pp), mobile-money credit use (+2.3 pp), and reported the platform feels safer (+5.3 pp). When people can tell legitimate contact from fraudulent contact, they engage with confidence rather than retreating in fear.

Cost-effectiveness and scalability

Scaling to Uganda's 11.4 million reachable mobile money users (at 72.7% completion) would prevent an estimated **160,000–205,000 fraud cases per year, saving consumers USD 3.5–4.5 million annually** from direct losses alone. Implementation costs hinge on one decision: zero-rating.

Scenario	Annual cost (Uganda scale)	Benefit–cost ratio
Zero-rated delivery	~USD 30,000	117 : 1 to 150 : 1
Commercial SMS rates	~USD 789,000	4.4 : 1 to 5.7 : 1

Table 2. Cost-benefit estimates based on direct fraud reduction only. Ratios exclude secondary benefits from increased DFS adoption, financial health, and complaint-driven market intelligence.

Implications for the global anti-scam community

1. Shift consumer protection budgets from information to capability. Awareness campaigns built on tips and warnings deliver small effects that fade within months, and—as our SMS test showed—information alone doesn't translate into action without underlying skill. Practice-based learning with feedback should become the standard, not the exception.

2. Sequence interventions: train first, then activate. Reminder SMS, in-app alerts, and provider warnings work only when people already know what to do with them. Sending the message before building the skill produces little of the intended response—and as our SMS test showed, can produce nothing at all. Build the skill first, then layer reminders on top.

3. Mandate or facilitate zero-rated delivery of fraud-prevention content. Zero-rating shifts benefit–cost ratios from 4:1 to over 100:1. Regulators and anti-scam coalitions should treat zero-rating agreements between MNOs and consumer-protection platforms as consumer-protection infrastructure, on par with KYC and AML obligations.

4. Use IVR and voice as inclusion infrastructure. Audio over basic phones reaches low-literacy and non-smartphone users that text-based campaigns systematically miss. Viamo already operates in 29 countries and 66 languages; per-country contextualization costs only USD 20,000–35,000. The delivery channel is ready for global replication.

5. Close the complaint feedback loop. The intervention would generate ~114,000 additional fraud complaints annually at Uganda scale—major new market intelligence on fraudulent actors. The pipeline is only valuable if regulators process, publish, and act on complaints. Industry, regulators, and platforms should jointly invest in faster, more transparent complaints handling.