DECODIS

HENRY J. LEIR INSTITUTE
ADVANCING HUMAN SECURITY

Digital Portfolios of the Poor

Digital Trust Philosophies

Kenya
May 2026

Executive Summary

Uneven patterns in digital financial usage

- The most recent financial and digital inclusion data shows weakness in digital financial use despite widespread access to digital devices and broad use of digital applications. In Kenya, very few people do not use digital financial services. Yet few store money in digital tool – is this reflect a lack of digital trust?
- We asked ourselves whether and how digital trust may be driving patterns in digital financial usage and whether it applies across applications and segments.

Measuring and using digital trust philosophies

- We leveraged automated voice interviews and AI-powered text analysis with 992 Kenyan men and women across a range of northern and southern Indian states.
- The responses collected were largely open-ended voice responses, surfacing qualitative perspectives often drowned out in traditional quantitative surveys.
- For this study, it was important to have this type of "qualitative data at quantitative scale" to allow for an inductive analysis of how respondents voiced their own perspectives without pre-specification of responses. Yet it was also important to have a large sample to test where a type of response was idiosyncratic across a few respondents or across the entire sample.

What we found

- Across the four countries covered in this study – Nigeria, Kenya, India and Pakistan – there were three archetypes of digital trust philosophies: Assurance seekers, Protection seekers and Control seeker.
- Sixty percent of this Kenyan sample were revealed to be Control Seekers, the most aware and confident users of digital tools. This is the highest percent of these most confident digital users out of the four countries, which isn't surprising given the long history of digital financial use in Kenya. However, surprisingly, 39% were categorized as Assurance Seekers, the least risk aware and confident archetype. Only 1% were Protection Seekers, which are aware of digital risks but unsure of how to protect themselves.
- A key feature of how these pillars were defined in Kenya is the consistency across all archetypes of how they defined Risk Mitigation. All participants uniformly talked about verifying requests by unrecognized numbers and reporting fraud. For most, this type of mitigation was about mobile money wallets, and many cited the litany of warnings from M-PESA almost as if by heart. For this reason, Risk Mitigation was kept out of the clustering process that determined the archetypes.

Tested with digital providers

- Digital providers effectively leveraged user segments. We used Digital Trust Philosophy segments in workshops with three SACCOs on the verge of digitizing their services. These workshops stimulated a range of actions across the institution to serve all archetypes.

Table of Contents

I. Objectives of the Study

- Problem
- Objectives

II. Qualitative Data at Scale

- Trust is qualitative
- Data collection
- Using telephonic skits
- Qualitative analysis at scale

III. Digital Portfolios Sample

- Types of phone access, ownership and sharing
- Access to multiple devices
- Use of applications

IV. Deriving Philosophies of Trust

- Pillars of trust philosophies
- Segments based on trust philosophies
- Segments by pillar

V. Workshops

- Objectives
- Institutions

I. Objectives of the Study

Why did we embark on this research?

Digital Trust Deficits and Digital Financial Management

Daily mobile phone use has grown substantially across the Global South along with social media, videos, voice and text messages.

But use of digital financial tools has lagged.

There are differentiating patterns across countries:

Kenya
High uptake of digitally-enabled accounts and payment use cases; lower use of storing money digitally.

Nigeria
Growth in uptake of digitally enabled accounts; payments well behind Kenya but storing money is higher.

India
Uptake in digitally enabled accounts and payment use is weaker; storage is higher.

Pakistan
Uptake in digitally-enabled accounts, payments and storage are weak across the board.

Can these uneven patterns be explained by a digital trust deficit?

Digital financial services providers often lament that customers lack trust.
But digital trust remains poorly defined.

All data from Findex, 2024.

What we aimed to do

01 Develop a globally relevant framework of digital trust philosophies as described from the perspective of the actual and potential users.

02 Determine if there are commonalities across countries, segments, phone ownership or other digital service use.

03 Test whether these frameworks help digital service providers to generate ideas about how to increase trust

II. Qualitative Data at Scale

A new research method

Trust is a qualitative notion but to meet our objectives we need scale

We need qualitative data because:

- Trust is a nebulous, qualitative idea which needs to be described in an open-ended response.
- Quantitative questions ask respondents pre-conceived answers - we want to be open to new perspectives.

We need to ask open-ended questions like:

- **Whose responsibility** is it to make sure that users don't experience privacy breaches or security risks?
- **How do you think** security and privacy breaches happen?
- **What do you see** as pros and cons of using digital financial services?

But we need a large sample size because:

- We want to know if trust deficits differ systematically across segments.
- We want a large enough sample to have segments relevant to a wide range of digital financial service providers.

Data collection: Asynchronous surveys using IVR

What we do
- Asynchronous interviews
- Pre-recorded local language-speaking voice actors not AI generated audio questions

But don't you need to probe?
- Well-tested questions turns what might sound as a disadvantage into a benefit.
- Not having a live interviewer meant no interruption or social desirability bias.[2]

The benefit
- Open-ended responses across 1000 people in four countries.
- Long, meaningful answers. Much longer than a typical live interview average.[1]

We also use skits to increase qualitative depth

What we do

We record fictional audio skits that respondents listen to, then asking questions about their thoughts about the scenario.

Benefits:

- Skits let people discuss sensitive or abstract topics like trust in a depersonalized way.
- Nebulous concepts are made concrete.

[1]See Decodis and Brac University paper about enumerator interruptions in live phone interviews in Bangladesh. Link here

[2]See Bergen and Labonte. 2020. "Detecting and Limiting Social Desirability Bias in Qualitative Research." *Qualitative Health Research* April 30 (5)

Data collection: Using skits

SKIT EXAMPLE

We use 6 skits, each followed by 8 questions

In this skit, Peter goes to the market to buy a few items from Moraa, but later returns them when she refuses mobile money due to an outstanding mobile loan and insists on cash. He then chooses to buy the items elsewhere, where mobile money is accepted.

CTRL+click on the image to see online

Click speaker to listen to the mobile money scenario in Swahili

Note: Videos are for illustration and translation purposes. Respondents are only exposed to skits via phone call.

RESPONSE EXAMPLE

Listen to a response in Swahili

"If I were Peter, I would go to the nearest Mpesa and withdraw money and then pay for the goods in cash because Moraa already explained she had a debt on her phone" (Woman)

Data collection: Asynchronous surveys using IVR and web links

What we do

- Asynchronous interviews
- Pre-recorded local language-speaking voice actors (not AI generated voice questions)

But don't you need to probe?

- Well-tested questions turn what might sound as a disadvantage into a benefit.
- Not having a live interviewer meant no interruption or social bias.

The benefit

- Open-ended responses across 939.
- Long, meaningful answers. 3x longer responses than in a typical in person interview.[1]

[1]See Decodis & Brac University paper about enumerator interruptions in live phone interviews in Bangladesh. Link here

992 people interviewed in Kenya

7 survey modules

360 hours
of voice data collected

280 voice response questions

166 keypad response questions

Data analysis: Inductively identifying themes using grounded theory

Example of response Decodis gets and how we categorize

RISK MITIGATION

"I think Onyango's father is someone very informed because it should be that when you are being called from Safaricom office there is a number that they use to call you. And if there is a number different from that of Safaricom then you should not suppose to receive the call. It is your personal duty because Safaricom daily sends messages they announce do not accept: do not accept any number that calls you apart from the one that we tell you. That is why I don't know they are which people, but we were told they once worked with Safaricom but were fired, or someone can trace your number. I can tell people to have awareness on such kind of people by telling someone that."

PERSONAL RESPONSIBILITY

TYPE OF RISK

With hundreds of hours of open-ended response in hands, we begin to understand the data by looking at a subsample of the responses and creating categorical themes based on how respondents answer. We create categorical themes until "saturation," i.e. when no new themes are emerging from looking at additional data.

This is an example of how we manually code responses before the prompt-writing process.

Data analysis: Using prompt-writing to tag themes to each question

Using this method across a large sample tells us whether themes are prevalent and not isolated incidents.

Step 1

We write the prompt for a machine learning model to search the data.

Context
The following texts are responses to questions about the risks and benefits of WhatsApp for business, online banking, POS transactions

Task
Based on the context, tag the response to the appropriate category based on what the respondent says about the risks of using online banking, POS transactions or platforms like WhatsApp for business.

Categorization Scheme
UnauthorizedPlatformAccess* – Hacking of WhatsApp or bank accounts due to lack of 2FA, malware, or SIM swap.
CyberFraud* – Fears of hackers, phishing, impersonation calls, and information theft through digital channels. Identity&ProfileTheft* – Impersonation on platforms like WhatsApp, with fake profiles used to scam others. ConnectivityFailures* – Frequent loss of signal, network downtime, or poor internet disrupting transactions, causes anxiety.

Output Instructions
Label the response with the relevant category name as listed in the categorization scheme

Step 2

The model tags responses that allude to trust themes. In this case, tens of thousands of open-ended responses are tagged.

Step 3

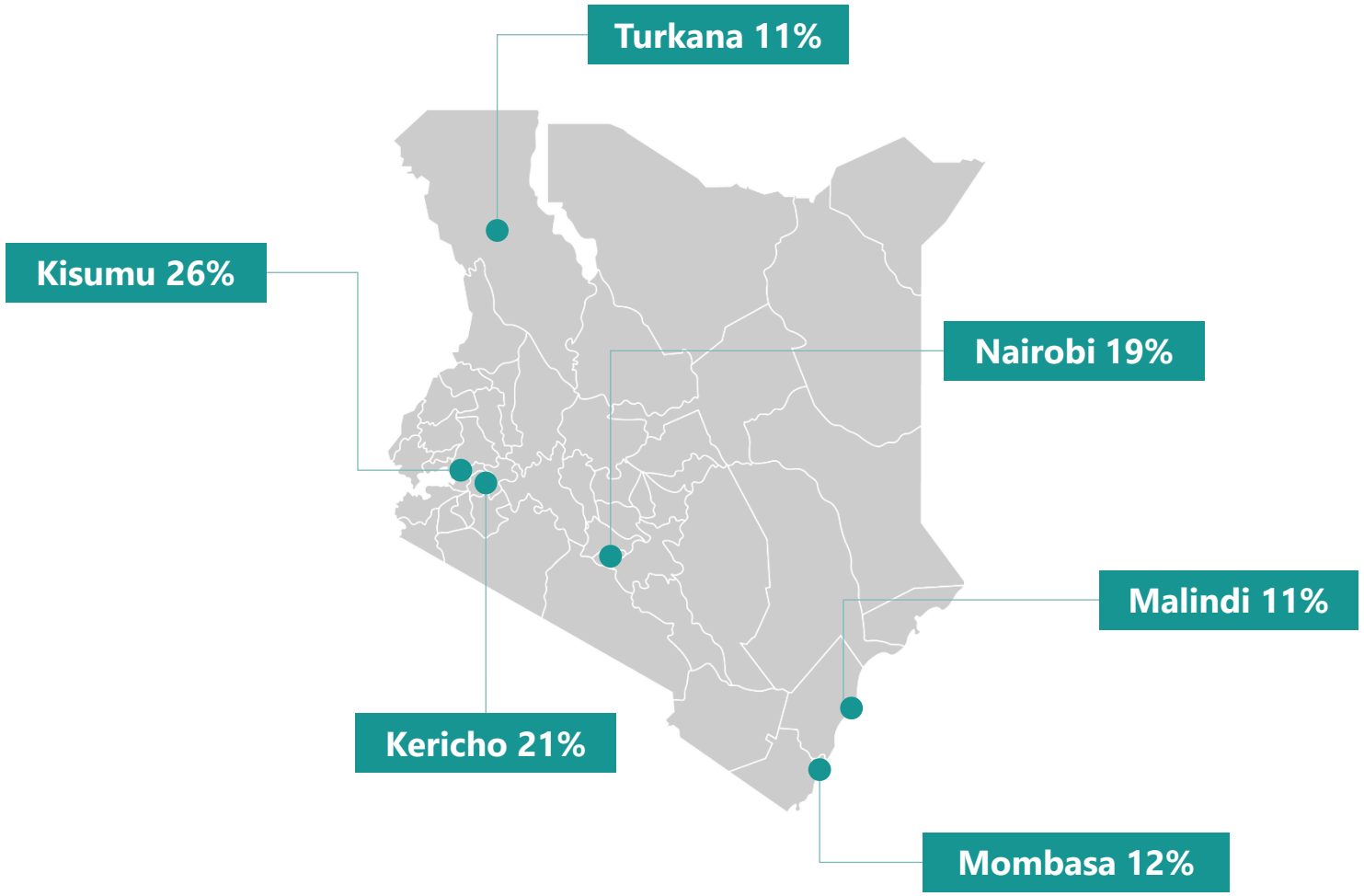
We do extensive iteration, improving the prompt and specificity of theme-tagging.

Resp ID	Transcription of response	Tags
Resp_001	**Someone has to be very careful while making online transactions or filling of forms.**	"Personal Responsibility"

III. Digital Portfolios Sample

Device and application use results for Kenya

Kenyan sample: Geographies and Languages



Key survey facts

- **Sample size**: 992
- **Languages**: Swahili, Luo, Kalenjin, Turkana
- **Data Collection:** October 2024

58%
Women

52%
26-35yrs

DECODIS

Kenya: Phone access and ownership

Reportedly high ownership[1], but more than half share any type of phone.

Reported Access v. Ownership	Smartphone	Feature phone	Basic phone
N (total 925)	618	273	34
Access to each type of phone	67%	30%	4%
Ownership of each type of phone	64%	27%	3%
↳ Owners who need to share phone	61%	57%	57%

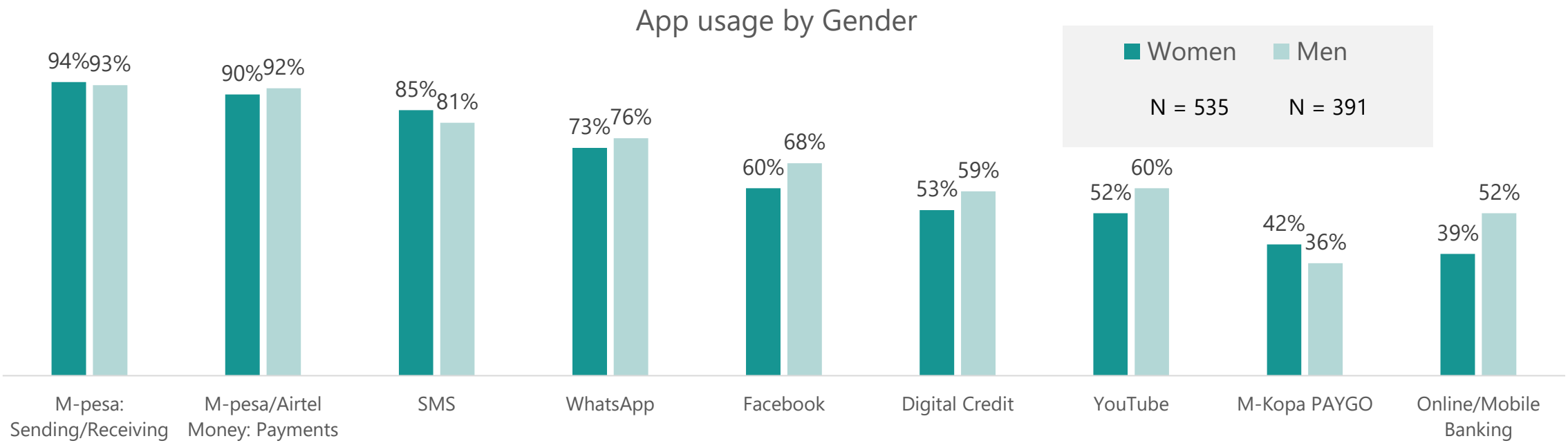
[1] Many respondents say they 'owned" their phones, but ownership has different definitions.

Most access to feature phones across the four countries, high reported ownership, lots of sharing

Nearly all women who had access to a particular type of phone said they owned it. However, we found through other questions in the survey that "ownership" is a broad idea. Many suggest that if they can use it, they feel a sense of "ownership." More importantly, over half of those who say they own their phones need to share with others in the household.

More surprisingly, 40% said they have access two devices and not just one (not shown here). However, we did not ask respondents to what degree they could access the second device. The responses could have ranged from being able to use it at any time compared to only using it briefly every now and then.

Kenyan sample: Types of digital use by gender



Generally, nearly all applications were used in equal proportions of men and women. However, a few data point deserve to be called out:

- Over 50% of men used online banking compared to 39%. This may be associated with a greater concern from women that the money saved digitally might be stolen.
- A larger proportion of women compared to men use M-KOPA as a strategy to purchase a smartphone, though digital credit, i.e. Fuliza is used more by men.

IV. Deriving Philosophies of Trust

in Digital Solutions and Archetypes

Our analytical process

IDENTIFYING **PHILOSOPHIES OF TRUST**	1	**1a** Inductively identifying trust themes and sub-themes using grounded theory
		1b Quantifying themes across the sample using prompt engineering
DERIVING **DIGITAL TRUST ARCHETYPES**	2	**2a** Deriving archetypes using cluster analysis
		2b Describing the archetypes
		2c Potential "typing tool" to put customers into archetypes

1 1a

Inductively derived pillars of digital trust

PILLARS OF DIGITAL TRUST

Together, these four pillars reveal **patterns of risk, responsibility, action, and reward** that create and maintain digital trust.

We extract themes of trust "inductively", which means **determined based on what respondents said** and not by forming hypothesis and looking for those in the data.

We derived four key pillars of trust grounded in participants' own words. It also generates a more comprehensive view of how underserved users approach digital engagement.

These pillars of digital trust are the same across all countries in the study.

Note: Risk Mitigation is not included in Kenyan archetype. While risk mitigation was included as one of the four pillars in our cluster analysis, in Kenya it did not meaningfully differentiate the clusters, as users across archetypes describe similar risk mitigation strategies despite differing in risk perception, responsibility, and benefit views.

1 1a

Sub-themes that define Risk Perception

A Risk Perception

Variable Name	Definitions
Scams	Respondents are concerned about fraud, fake schemes, and deceptive messages that try to steal money or information that would enable fraud. However, they also expressed "scams" as their own family or friends being able to get into their M-PESA account and steal money without them knowing it. This is most often expressed in the context of sharing phones.
Auto-deductions from credit	Respondents expressed an unusual perspective in Kenya: The risk of using digital credit, mostly Fuliza, and facing unexpected auto-deductions as a result.
Harassment	Respondents expressed concerned about harassment online – mostly women who do business on social media.
None	They cannot articulate particular risks and state that they know nothing to be concerned about.

In nearly all countries, digital scams of some type were at the top of the list of digital dangers. In Kenya, there were many mentions of scams from strangers, but also from family and friends who would steal from their mobile money wallets without them knowing. This fear did not come up in any other country.

Also, in the landscape of digital credit, respondents expressed the risk of money being auto-deducted unexpectedly and suddenly being left with nothing in their mobile money wallet. In an environment that has long been shifting towards a more digital financial environment, the challenge of suddenly not having money in an M-PESA account means not having available money at all.

1 1a

Sub-themes that define Risk Mitigation

B Risk Mitigation

Variable Name	Definitions
Verify	Users double-check messages and transactions, confirm numbers before sending payments, block or delete unknown contacts.
Report	Users talk about using official phone numbers or sanctioned channels to report fraud.
Passive	Users are passive about taking protective risks, assuming that they are protected by others (although they might not articulate by who).

Note: Risk Mitigation is not included in Kenyan archetypes:

While risk mitigation was included as one of the four pillars in our cluster analysis, in Kenya it did not statistically differentiate the clusters, as users across archetypes describe similar risk mitigation strategies despite differing in risk perception, responsibility, and benefit views.

A small number of respondents expressed a passive perspective on risk mitigation, believing they are somehow protected.

However, most other respondents talked about both verification and reporting scams. Most often, they recited recommendations about mitigating and reporting risks to do with M-PESA. For them, digital risks were monolithically about money.

1 1a

Sub-themes that define Responsibility Perception

C Responsibility Perception

Variable Name	Definitions
Government	Government is responsible for making the digital world safe.
Self-protection	It is every user's own responsibility to ensure the security of their device or accounts.
Telecoms companies	It is the telco provider's (Safaricom) duty to protect customers.
Unsure	They do not know whose responsibility it is to ensure digital safety.

These categories of Responsibility Perception are generally the same across countries.

However, given the long experience with M-PESA in Kenya by most of the population, digital risks are associated with mobile money, and mobile money means Safaricom. Many respondents gave the Safaricom call center phone number in their responses and dutifully listed instructions about preventing scams they have undoubtedly heard many times.

1 1a

Sub-themes that define Benefit Perception

D Benefit Perception

Variable Name	Definitions
Financial Access	Digital financial services provide quick access to money, including but beyond business needs.
Market Reach	Digital channels open greater reach for business and opportunities.
Self Reliance	Respondents say they can do things for themselves through their phone – whether it's conducting business or accessing services – independently and privately.

Market Reach is a consistent benefit expressed across all four countries.

However, in Kenya, self-reliance was a theme that was brought up by a wide range of the respondents. Kenyans in this sample talked about a sense of pride that they could do things for themselves on their phones. One topic they spoke about was knowledge-seeking, i.e. the ability to simply build their knowledge when and how they wanted.

A set of globally-relevant Digital Trust Philosophy archetypes

AS

Assurance seekers

They have limited understanding of risks and mitigation, building trust through peer assurance.

PS

Protection seekers

They have the widest range of fears, increasing the likelihood of withdrawing from digital tools. They build trust through provider or government protection.

CS

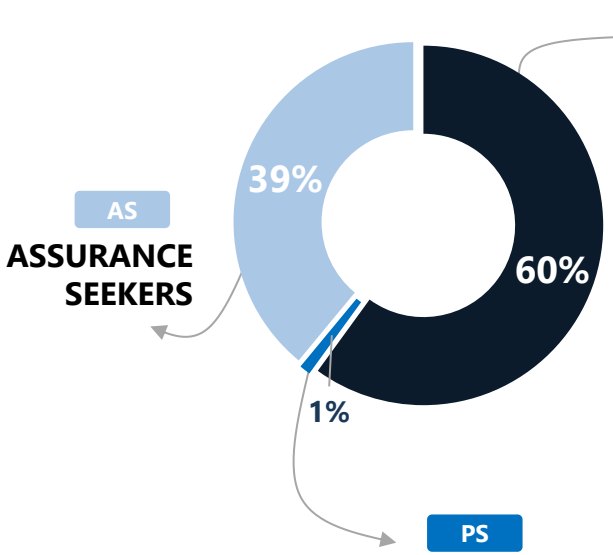
Control seekers

Digitally competent and confident in their ability to self-protect

Kenya: Proportions of archetypes

Archetypes in Kenya

N=992



AS
ASSURANCE SEEKERS

"Stuck in the past" with focus on mobile money rather than other digital tools. Focused on the benefits of DFS as being part of the financial world and moving money around. Little understanding of what risks there are and who is responsible for protecting them.

CS
CONTROL SEEKERS

Highest users of a range of digital financial services. They are concerned about scams in general, but **mostly with reference to someone stealing from their wallet**. They speak about government providing them safety digitally, but this is mostly with respect to providing safety for women being harassed on the internet.

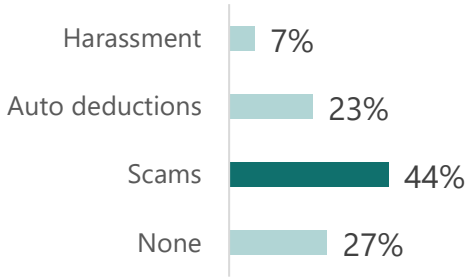
PS
PROTECTION SEEKERS

There are very few Protection Seekers in the Kenyan sample, characterized mainly by an expectation for Telcos to protection their online lives. This reflects a bifurcation in the sample based on who holds responsibility for digital risk. There is very little discussion in the overall sample about Telco having responsibility. This may reflect experiences of long-term mobile money use.

Assurance Seekers: Attributes

Of those who are Assurance Seekers and talking about each pillar,
% who mention this type at least once

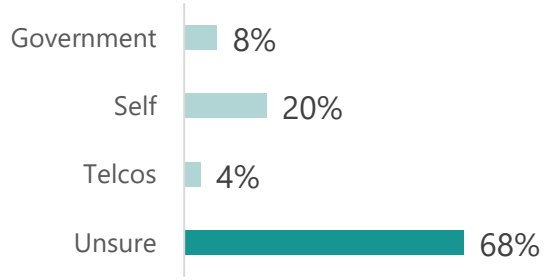
A Risk Perception



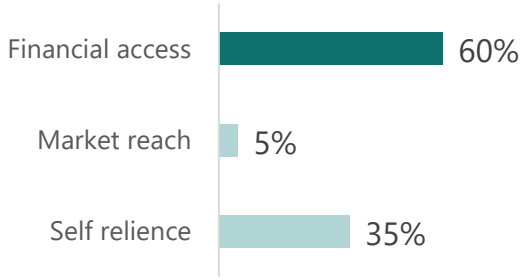
B Risk Mitigation

Not applicable in Kenya

C Responsibility Perception



D Benefit Perception



AS ASSURANCE SEEKERS
39% of the sample

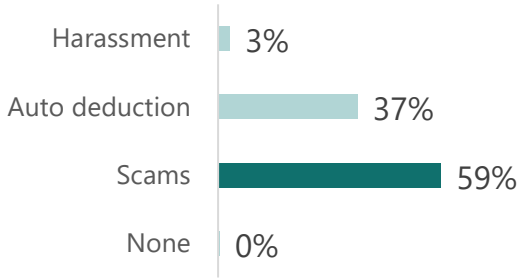
- 53% of this archetype are women.
- 61% have access to a smartphone.
- 58% need to share the phone.
- "Stuck in the past" with more use of mobile money than other digital uses
- Benefits are focused on financial access.
- Trust is tentative, being unsure of who bears the responsibility of protection
- Risk of financial scams is expressed as a fear that someone will steal from their mobile money accounts.

"I don't want anybody to know my bank, my account, or how I operate my account . **Because they may steal my money in the bank account**."
26-year-old male, Turkana County

Protection Seekers: Attributes

Of those who are Protection Seekers and talking about each pillar,
% who mention this type at least once

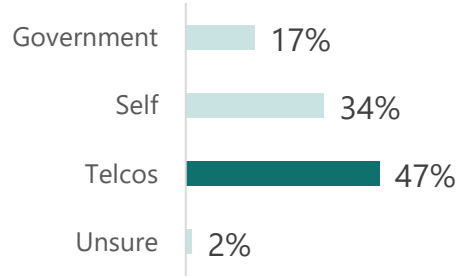
A Risk Perception



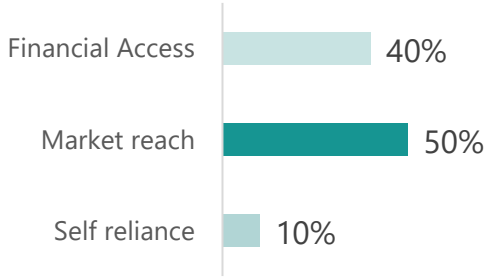
B Risk Mitigation

Not applicable in Kenya

C Responsibility Perception



D Benefit Perception



PS PROTECTION SEEKERS
1% of the sample

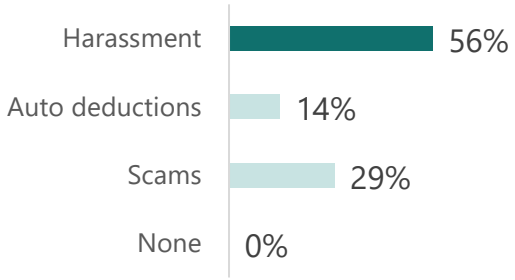
- Very few respondents.
- The only archetype that feels Telcos have responsibility for protecting them.

"**Service providers or social media service providers are the ones who should ensure that every person should be able to do business especially.**"
34 year old Male, Kericho

Control Seekers: Attributes

Of those who are Control Seekers and talking about each pillar,
% who mention this type at least once

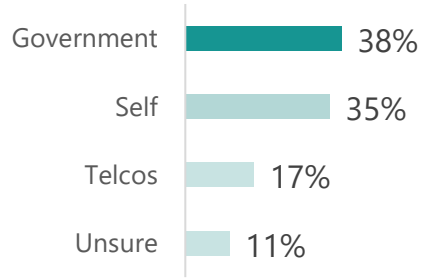
A Risk Perception



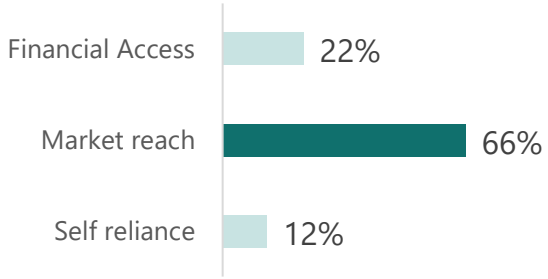
B Risk Mitigation

Not applicable in Kenya

C Responsibility Perception



D Benefit Perception



CS CONTROL SEEKERS

60% of the sample

- 51% of this archetype are women.
- 61% have access to smartphones.
- 52% need to share the phone in some way.
- They are deeply embedded in their digital lives, especially in using social media for business
- Given their deep engagement in the digital world, they are most concerned about harassment
- They rely on themselves to protect themselves online, but many express a desire for the government to protect their safety online.

"It is the duty of the government to ensure everyone has access and freedom to do business as they would prefer according to their abilities. So **if women are being abused on the internet ,then the government needs to be alert to ensure it sorts abuse of women** so that women can progress. "
44 year old Female, Malindi

Key questions institutions can use to type customers into trust archetypes

In order to understand which archetype a customer fits within the most, they can be asked this set of questions.

1. **What type of device do you mostly use?**
2. **What types of digital services do you use?**
3. **What do you see as risks of digital services?**
4. **Who do you think is responsible for protecting you from digital risks?**
5. **What are the greatest benefits of digital channels for you?**

Based on their open-ended response, themes can be extracted using pre-built code.

V. Workshops in Kenya

Did this research influence how providers could build trust in digital channels?

Objectives of the workshops

Objective 1

Solve for more than one archetype

- **Identifying customer types easily** - if institutions need to type customers themselves, this would be burdensome
- **Solve for trust archetypes that they already have**, even if not explicitly typified
- **Solve for more than one type of customer** to meet multiple trust needs
- **Solve for a concrete set of attributes.**

Objective 2

Lessons to generate tractable actions across departments

- **Proposing different solutions to earn a slot in the pipeline:** Because there are constant projects and priorities happening across departments, there needs to be a multitude of solutions in order for at least some to enter the project pipeline.
- **Start with low effort to gain traction:** Not all solutions need to be complicated – being able to implement some "low-hanging fruit" provides evidence to invest in more complex solutions
- **Create solutions for different trust needs:** Multiple changes implemented across aspects of customer experience will be more effective at growing customer trust than just one

Keys to success

Attendance

- **Must have senior people** from product development, communications, etc.
- **Must only take half a day** so it is easy for those people to attend

Rotate experience of solutioning for archetypes

- **Work with 2 most prevalent archetypes** in country
- If possible, it is helpful to **have examples of the archetypes** from their customer base
- **The "why" of the workshop**: Your customers are not monolithic in terms of their trust deficits. As you won't know what the trust philosophies are (because they are hidden), you need to "cover all the bases"
- **Workshop participants work with both archetype** to drive home how different archetypes focus on different types of risk.
- An exercise that leads back to normal life – **end with a concrete pitch**

Workshop Process

Framework Introduction

Key outcome: Get situated

We present study findings to expose workshop attendees to the concepts of trust philosophies

Then, we explain the three archetypes and the four trust pillars. Pick two archetypes.

1 Problem Identification

Key outcome: Articulate key pain points of each archetype with respect to their product

We split attendees into small groups, assigning each an archetype. Groups role-play customers and list product pain points and barriers. This allows them to compare how the problems manifest differently across archetypes.

2 Solution Identification

Key outcome: Create cross-institution

Co-design cross-functional solutions. Teams come up with a prioritized set of archetype-aligned solution themes.

3 Make it Actionable

Key outcome: Create proposals of the business

Produce concrete proposals (short, medium and long term), measures of success and next steps.

7 prompts:

- Tell me about your customer (archetype)
- Tell me about their problem
- How would you solve with $100,000?
- What actions (short/medium/long term)?
- How will you measure success?
- How will you ensure lasting impact?
- Summarize as an evocative story

Workshop institutions

Stima is a leading SACCO in Kenya serving employees in the energy sector and their dependents. They are known for its large asset base, national reach.

They are early adoption of digital platforms to deliver financial services

Shirika is growing SACCO primarily serving civil servants across Kenya. It has a diverse and expanding membership.

They are actively investing in digital transformation to better reach and retain members.

Mwalimo is the largest SACCO in Kenya by membership, focused on teachers and education sector workers. It has deep rural penetration and a strong legacy presence.

They have efforts underway to modernize member services through digital channels.

Why we work with SACCOs:

- They service bottom of the pyramid
- They are only just starting to design digital channels
- They rarely have this type of workshop.

Workshop institutions: Stima SACCO

Institution’s objectives

Stima's priorities: concrete, gender-sensitive design choices and measurable pilots that advance poverty reduction and gender equality.

They want the session to help them align product features with SDG goals, prevent unintended exclusion, and design scalable interventions to reach the most vulnerable women.

11

Teams represented

- FOSA
- Finance
- Shared Service
- Marketing
- Sales, Research
- Treasury
- Customer Experience
- Credit
- ICT
- Legal
- Management

Stima Outputs

	1 Problem Identification	2 Solution Identification	3 Make it Actionable
CS **CONTROL SEEKERS**	• Limited personalization that fails to reflect cashflow rhythms • Lack of configurable alerts, limits, and visibility undermines perceived control and financial safety • Opaque processes reduce use by users who demand auditability	• In-app dispute clarity button linked to CRM • Members can track/clear loan issues seamlessly • Flexible repayment options(daily/weekly)	**Legal/Compliance** • In-app dispute clarity button linked to CRM • Members can track/clear loan issues seamlessly **Branch/Finance** • Flexible repayment options(daily/weekly) • Apple Store-style genius bar for hands-on support **Customer Experience** • Community Q&A support button • App-based loyalty/referral incentives • Offline access and local reassurance are essential for vulnerable members
AS **ASSURANCE SEEKERS**	• Many remain on USSD or offline channels and lack confidence in apps or digital privacy • Need reputation-building incentives and simple conversion paths that do not exclude low-literacy users	• Apple Store-style genius bar for hands-on support • Community Q&A support button • App-based loyalty/referral incentives • Offline access and local reassurance are essential for vulnerable members	

Workshop institutions: Shirika SACCOs

Institution's objectives

Translate DPP insights into practical, trust-aware strategies that help Shirika close the generational gap—attract younger members while keeping older members comfortable—and increase uptake of digital services despite concerns about reliability, privacy, and digital literacy.

The focus is on modernizing service delivery in ways that protect and amplify Shirika's long-standing reputation.

9

Teams represented

- Senior Leadership
- Treasury
- Credit
- Marketing
- HR
- ICT
- Customer Experience
- Internal Audit
- Accounts

Shirika Outputs

	2 Problem Identification	3 Solution Identification	4 Make it Actionable
CS **CONTROL SEEKERS**	• Lack of consolidated, reliable loan information deters confident self-navigation • Need round-the-clock access to digital updates to reduce dependency on branch visits • Digital gaps in transparency limit appeal to younger, tech-savvy members	• Standardized digital loan checklists for consistent understanding across age groups • Real-time status updates to keep members informed and reduce anxiety • Self-assessment eligibility checker tool allows members — especially younger users — to verify loan fit independently	**Internal Audit** • Standardized digital loan checklists for consistent understanding across age groups **Credit/ICT** • Self-assessment eligibility checker tool allows members.— especially younger users — to verify loan fit independent
AS **ASSURANCE SEEKERS**	• Older or less digitally confident members struggle to find relatable success stories • Trust builds through peer experiences, not technical explanations • Lack of accessible, plain-language guidance limits confidence in new platforms	• Onboard new members with short surveys to surface concerns early • Create a repository of real user stories to serve as social proof • Deliver FAQs and info sessions in plain, jargon-free language	**Marketing/Customer Experience** • Onboard new members with short surveys to surface concerns early • Create a repository of real user stories to serve as social proof • Deliver FAQs and info sessions in plain, jargon-free language

Workshop institutions: Mwalimo National

Institution's objectives

Apply DPP insights to the unique financial journey of teachers — characterized by salary-linked cash flows and a fragile transition at retirement.

The goal was to identify key trust touchpoints and translate them into practical solutions that strengthen digital confidence and improve member retention beyond active employment.

5

Teams represented

- Business innovation
- HR
- ESG
- Marketing
- Customer Experience

Mwalimo National Outputs

	2 Problem Identification	3 Solution Identification	4 Make it Actionable
CS **CONTROL SEEKERS**	• App limited to wallet transfers and lacks features that reflect salary cycles and retirement needs • No single place to view loan, savings, and retirement status across the member journey	• Run new-member surveys on salary cycles, retirement plans, and product needs; use insights to inform design • Integrate loan, savings, and pension tools into one platform with status tracking • Pilot insurance or pension safeguards; track uptake and retention of retiring members	**ESG** • Run new-member surveys on salary cycles, retirement plans, and product needs; use insights to inform design **Marketing & Customer Experience** • Pilot insurance or pension safeguards; track uptake and retention of retiring members • Set referral targets tied to onboarding to surface credible peer stories for hesitant members **Business Innovation** • Integrate loan, savings, and pension tools into one platform with status tracking • Use member referrals and targeted testimonial campaigns to build trust during retirement transition
AS **ASSURANCE SEEKERS**	• High churn driven by reliance on peers' experiences and fear about post-retirement financial stability • Low confidence in app-based services; prefer reassurance from other members or staff • Lack of visible, relatable proof that services protect members after employment ends	• Use member referrals and targeted testimonial campaigns to build trust during retirement transition • Set referral targets tied to onboarding to surface credible peer stories for hesitant members • Maintain consistent, friendly engagement (offline + low-tech channels) to reassure older or retiring teachers	

VI. Conclusions

What did we learn?

Conclusions

- Inductive analysis of digital trust across four countries manifested four common pillars, which statistically clustered into three archetypes.

- In this Kenyan sample, over half were in the Control Seekers archetype. These are users who are most aware of digital risks and are the most confident – indeed, downright nonchalant – about using digital strategies to mitigate them.

- At the other end of the scale are Assurance Seekers, which make up a surprisingly large 39% of this sample. A large percentage of these users, 27%, cannot articulate or name digital risks, These users are fully aware of digital risks and

- 68% are unsure of who should be responsible for protecting them digitally. Within the Kenya context of nearly ubiquitous use of M-PESA and a higher prevalence of feature phones than the other three countries, this archetype reflects Kenyans who are "stuck in the past" and haven't moved beyond using M-PESA for their basic remittance needs.

- With these two completely different archetypes dominating the Kenyan landscape, what are digital financial providers to do to grow trust with both? By focusing on SACCOs, who are increasing introducing digital tools, we anticipated that a sizable portion of their customer should be Assurance Seekers keeping to community-oriented financial institutions, while knowing that they surely would also have Control Seekers, given how prevalent they are in the Kenyan population. By using details of both archetypes, each institution was able to brainstorm solutions that would serve each across their various departments.

Annex

A new analytical lens: Assessing trust philosophies

- Traditional segmentation: Measures who is digitally active, and why.
- Most digital inclusion research uses inductive segmentation: grouping users by *who uses what*, *how often*, or *on which channels* — and then crafting interventions to move users "forward" on some digital journey.
- This approach is useful for mapping activity, but it reveals little about the *why* and *how* behind digital behaviors.
- Digital engagement is not only about access or skills. It's fundamentally about trust — how users perceive risk, build confidence, and decide to engage or withdraw.
- Inductive "usage" segments miss the *invisible architecture* of trust:
    - Two people might both use mobile money, but one does so only after triple-checking with their bank and friends, while the other simply accepts things as they are.
    - Standard segments would group these two together, missing the *radically different trust philosophies* — and, therefore, the different types of support they need.
- Inductive analysis unearths *not usage profiles*, but *trust philosophies* shaping every digital action, risk, and expectation.
- Inductive segmentation makes the digital landscape look flat. Trust philosophy segmentation reveals its contours. Each group looks similar on the surface, but their risk perceptions, barriers, motivators, and intervention needs are fundamentally different.

Our approach is different

We start by listening for how users *perceive*, *manage*, and *act upon* trust and risk, capturing responses in four critical areas:

- Risk perception: What are people truly worried about? (e.g., hacking, scams, failure, theft)
- Risk mitigation: What do people *actually do* to protect themselves? (e.g., external confirmation, cautious sharing, monitoring)
- Responsibility perception: Who do they believe should keep them safe — institutions, platforms, themselves, or others?
- Benefit perception: What makes digital services worth the risk? (e.g., time saved, income, ease, safety)
- By collecting data across these four windows into their lived realities, we ran a cluster analysis that looks beyond what people do and reveals *how* and *why* different people *trust*.
- The method uncovers *natural groupings* — segments are not forced but emerge based on patterns in how people weigh risk, take precautions, assign responsibility, and see value.
- Each cluster is a distinct trust profile: Not just a behavioral group, but a reflection of a deeper, guiding trust philosophy —
    - Some users only trust after actively checking and verifying.
    - Others simply accept digital risk as a fact of life.
    - Another group pursues inclusion on their own terms, by taking personal control.
- By identifying these unique trust and risk management philosophies, practitioners and designers can build interventions, protections, and communications that resonate — "speaking the language of trust" that users actually use.

Analysis steps

1. **Multi-dimensional Data Integration:** We systematically synthesize respondents' open-ended responses to questions across four core dimensions: *Risk Perception, Risk Mitigation Behaviors, Responsibility Perception and Benefit Recognition. This ensures a holistic capture of trust-related attitudes and behaviors.*

2. **Thematic Analysis – Systematic Inductive Coding:** Using iterative, grounded coding techniques, we inductively identify thematic categories and subcategories across all four pillars. This qualitative approach unravels not only surface concerns, but also latent, recurrent themes embedded in diverse user experiences.

3. **Latent Profile Derivation through Qualitative Comparative Patterning:** We conduct cross-sectional pattern analysis across coded data to qualitatively derive emergent trust profiles, identifying meaningful clusters of respondents based on distinct patterns of trust formation, risk response, and benefit expectation.

4. **Empirical Validation via Agglomerative Cluster Analysis:** To validate and solidify the qualitative typology, we employ agglomerative hierarchical clustering to empirically test the robustness and reproducibility of the emergent clusters along the full suite of coded variables.

Why do we choose the four factors we do to define our trust philosophies?

1. **Risk Perception:** Trust begins with awareness. People's readiness to use digital tools depends on what dangers they foresee, whether that's hacking, scams, or technical failures. Mapping risk perception allows us to capture why some users hesitate while others proceed—revealing the emotional and cognitive triggers that open or close the door to digital adoption.

2. **Risk Mitigation:** Trust is more than belief; it is enacted through daily choices. By examining risk mitigation strategies—like cautious sharing and external verification—we get granular insight into how users translate their fears or confidence into practice. This dimension reveals not just theoretical trust, but trust-in-action.

3. **Responsibility Perception:** Trust is deeply social and institutional. Whether users trust a system often hinges on *who* they believe is accountable for security—banks, government, platforms, or themselves. By including responsibility perception, we surface the implicit contracts and expectations that frame people's willingness to engage.

4. **Benefit Perception:** Trust is not only about reducing risk, but about pursuing value. Users weigh risks against perceived benefits: income opportunities, convenience, safety, or cost savings. This dimension grounds trust in lived realities and practical utility—capturing why digital services are worth the leap of faith.

DECODIS

Social Research. Reimagined.

linkedin.com/company/decodis

@decodisresearch

@decodisresearch

info@decodis.com

www.decodis.com