Reducing Non-Institutional Fraud and Building Trust in a Digital Market Platform: Evidence from a Field Experiment in Nigeria

Pre-Analysis Plan

Chaning Jang, Michael King and Daniel Putman

The high prevalence of digital financial fraud makes it difficult for businesses to distinguish between real communications from digital service providers and fraudulent communication. This could lead to a lack of trust in, and usage of digital financial services. Through a field experiment and a combination of administrative data and self-reported responses, we test two strategies for preventing non-institutional fraud: an anti-fraud campaign and a technical intervention – a unique communications code – which verifies the provenance of messages sent from a digital platform. First, we assess whether these anti-fraud interventions reduce susceptibility to fraudulent communications, and confidence in one's ability to avoid fraud. Second, we test how these interventions affect trust in, and usage of financial services. We analyze how these impacts differ within key subgroups, including by demographic characteristics, socio-economic status, and risk preferences. Findings from this study will help improve consumer protection and support digital security in the financial and non-financial service sectors.

Contents

1. Introduction

Non-institutional fraud targeted at micro, small, and medium enterprises (MSMEs) is pervasive across low- and middle-income countries (LMIC) and has risen in the wake of the COVID-19 pandemic.[1] Not only can fraud lead to immediate (and sometimes severe) monetary and psychological damage, it can lead to systemic mistrust in, and underuse of digital services. There is limited knowledge on what mitigation strategies can be taken to reduce fraud and help bring the promise of digital financial services to MSEs in developing countries. This project seeks to address this gap by understanding the impact of i) a learning intervention aimed at consumer capacity to distinguish between fraud and legitimate communication and ii) a unique customer code (UCC) on trust in digital services.

The concept of non-institutional fraud covers a range of potential activities, including phishing[2] scams to access passwords and log-ins, impersonating a formal institution, offering fake products or services and absconding with payments, and using psychological manipulation to persuade victims to part with money.[3] Non-institutional fraud is carried out by individuals or groups who are not affiliated with a formal institution (i.e. not insiders in a bank or affiliate) who seek to trick victims into directly sending money, or sending sensitive information that can be used to defraud the victim.

Non-institutional fraud is pervasive: IPA's recent consumer protection surveys in Kenya, Nigeria and Uganda found that phishing scams had been faced by 56% of Kenyan respondents, 33% of Ugandan respondents, and 42% of Nigerian respondents. This was the most prevalent issue in Kenya and Uganda, and the third most prevalent in Nigeria.[4] MSEs are common targets of non-institutional fraud in developing countries, despite perceptions that fraud is targeted at larger businesses.[5] MSEs face fraud risk related to their customers, and also their employees, and have multiple vulnerabilities including business bank accounts, purchases and sales transactions, and business IT infrastructure.

Non-institutional fraud causes immediate and long-term damage. Immediately, fraud leads to monetary loss, but also to psychological impacts including anger, difficulties with trust, feelings of violation, stress, and social embarrassment.[6] In the long-term, low trust may lower willingness to access digital financial services (DFS). This is damaging for MSEs in particular, as digitalization can drive access to market through platform engagement and social media, and access to finance through new digital finance

[1] Tade, Oludayo. "Social Context of Cybercrime in the Age of COVID-19 in Nigeria." *African Security*, 2021 1–24.

[2] Phishing refers to the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

[3] Garz, Seth and Gine, Xavier and Karlan, Dean and Mazer, Rafe and Sanford, Caitlin and Zinman, Jonathan, Consumer Protection for Financial Inclusion in Low- and Middle-Income Countries: Bridging Regulator and Academic Perspectives, Annual Review of Financial Economics, 2021.

[4] Blackmon, William, Rafe Mazer, and Shana Warren. 2021. "Kenya Consumer Protection in Digital Finance Survey." Blackmon, William, Rafe Mazer, and Shana Warren. 2021. "Nigeria Consumer Protection in Digital Finance Survey." Bird, Matthew, and Rafe Mazer. 2021. "Uganda Consumer Protection in Digital Finance Survey."

[5] Salah Kabanda, Maureen Tanner & Cameron Kent (2018) Exploring SME cybersecurity practices in developing countries, Journal of Organizational Computing and Electronic Commerce, 28:3, 269-282.

[6] DeLiema, Marguerite and Mottola, Gary R. and Deevy, Martha, Findings from a Pilot Study to Measure Financial Fraud in the United States (February 9, 2017).

opportunities.[7] Notwithstanding regulatory differences, the lower rate of digital payments in Nigeria compared to Kenya may reflect lower levels of trust in digital financial services.[8]

Based on the modus operandi of fraudsters, several strategies are often pointed to in preventing its negative ex post effects. We consider two of these strategies: financial literacy interventions and a technical intervention – a unique communications code – which verifies the provenance of messages sent from a digital platform. Using a randomized evaluation and self-reported outcomes, we test whether repeated exposure to a financial literacy intervention from a digital market platform reduces susceptibility to fraud among MSMEs. Similarly, we test how the UCC empowers MSMEs to avoid fraudulent communications. We test the effects on confidence in identifying fraud and trust in DFS. Finally, using self-reported outcomes and administrative data from a digital market platform, we test how these interventions impact usage of DFS.

Conducted in partnership with Amana Market, a digital platform in Nigeria that offers access to market information, trading options and financial services to MSEs, this study involves a randomized evaluation with users of the platform across three states in Northern Nigeria: Kaduna, Kano, and Jigawa. MSEs will be randomised into one of three groups; a control, a financial education arm, or the UCC arm. Participants will answer a short baseline survey and a more extensive endline survey to measure a range of outcomes around susceptibility to fraud, trust in platforms, and engagement with the platform. Additionally, to understand usage of digital financial services, we will draw on participant's administrative data from the Amana Market platform. We anticipate that findings from this study will help improve consumer protection and support digital security for Africa's large and growing market platform and financial services sectors.[9]

2. Research Questions

There are eight core research questions to be answered by the field experiment.

1. Do anti-fraud interventions affect MSEs susceptibility to fraudulent communications?
2. Do anti-fraud interventions affect MSEs ability to detect fraudulent communications?
3. Do anti-fraud interventions affect confidence in one's ability to distinguish between genuine and fraudulent communications?
4. Do anti-fraud interventions affect knowledge about types of fraudulent communications?
5. Do anti-fraud interventions affect trust in digital financial services, and specifically in Amana Market?
6. Do anti-fraud interventions affect usage of digital finance services, and specifically Amana Market? Do such interventions have increasing or diminishing effects over time?

[7] Partnership for Finance in a Digital Africa, "Micro-entrepreneurs in a platform era," Farnham, Surrey, United Kingdom: Caribou Digital Publishing, 2019. https://mse.financedigitalafrica.org.

[8] World Bank Group. 2019. Nigeria Digital Economy Diagnostic Report. Washington, DC: World Bank. License: Creative Commons Attribution CC BY 3.0 IGO

[9] Online marketplaces which facilitate commercial transactions between buyers and sellers.

Additionally, we have two supporting research questions related to the heterogeneity of effects:

7. Does experience with ICTs, DFS, or past fraud attempts serve as a substitute or complement to the anti-fraud interventions?
8. Are anti-fraud interventions equally effective for subgroups with different demographic characteristics and preferences, such as female-headed businesses, older business owners, those of lower socioeconomic status, or those who are more willing to take risks?

3. Research Strategy

Outcome measurement

Fraud Victimization, Knowledge, and Detection

Participants are asked to report if they have encountered fraudulent communications. If they have, respondents are asked if they complied (or engaged with) with the fraudster. If they complied, they were asked if they suffered losses. Of these three levels of fraud exposure we take compliance and losses to be tiered levels of victimization of fraud. While our ultimate goal is reduction in fraud victimization among MSEs, we are cognizant of the limitations of measuring reductions in victimization given that victimization is a rare event.[10] Depending on the overall prevalence of compliance and losses, we will explore outcome measures that best capture the margin where we are powered to detect abatement. For example, if very few people have lost money, but more have complied with fraudsters, our primary measure of victimization will be compliance. In this case, losses will be a secondary measure.

In addition to fraud victimization, the survey will elicit self-reports about the respondents confidence in detecting fraud. Finally, we will use two separate five question quizzes to get a sense of knowledge about fraud and fraud detection ability.

Table 1: Outcomes related to fraud detection and victimization

Outcome	Tier	Type	Details
Compliance	Primary or Secondary	Survey	An indicator variable equal to one for those who were contacted and complied with the scammer. Depending on the number of people who have lost money, we may opt to choose compliance as the primary.
Losses	Primary or Secondary	Survey	An indicator variable equal to one those who incurred losses. Tier is the opposite of compliance.

[10] Suppose, for example, we are able to reduce victimization by 10%. That is, 10% of people who might be victimized are not because of our training or UCC. In a population where 50% of people are victimized by fraud, this is an effect size of 5 percentage points, while in a population where 5% are victimized, it is half a percentage point.

Confidence	Primary	Survey	An Inverse Correlated Weighted Index of self-assessments of confidence in identifying the provenance of communications.
Detection	Primary	Survey	Score in five question quiz
Detection Confidence	Secondary	Follow-up Quiz	Average self-reported confidence in ability to detect fraud in quiz.
Knowledge	Primary	Survey	Score in five question quiz

Trust and usage of digital financial services

Endline surveys will be conducted to allow us to test several key research questions, namely, does the financial education intervention in the experiment impact trust in and willingness to use DFS? These outcomes will come from both self-reported survey measures and administrative data from Amana Market. These outcomes are listed in Table 2.

Table 2: Outcomes related to trust and usage of DFS

Outcome	**Tier**	**Type**	**Details**
Amana Market Usage - Binary	Primary	Admin	An indicator variable equal to one if the participant transacted on the Amana Market platform in the last six months of the experimental period, and zero otherwise.
Amana Market Usage - Total Transacted	Primary	Admin	A variable that will track the total amount transacted in the last six months of the experiment. This will equal zero if they have not transacted using the service.
Self-Reported Usage	Primary	Survey	Index of usage for six types of digital financial services.
Index of trust - DFS	Primary	Survey	Inverse Correlation Weighted Index of trust in DFS outcomes.[11]
Information - DFS	Secondary	Survey	Self-reported agreement that their information is kept safe by a variety of DFS providers, on a scale of 1 (strongly disagree)-7 (strongly agree)
Money - DFS	Secondary	Survey	Self-reported assessment money is kept safe from fraud when using a variety of DFS providers, on a scale of 1 (strongly disagree)-7 (strongly agree)
Index of trust - Amana Market	Primary	Survey	Inverse Correlation Weighted Index of trust in Amana Market
Information - Amana Market	Secondary	Survey	Self-reported agreement that their information is kept safe by Amana Market, on a scale of 1 (strongly disagree)-7 (strongly agree)

[11] Anderson, Michael L. "Multiple Inference and Gender Differences in the Effects of Early Intervention: A Re-evaluation of the Abecedarian, Perry Preschool, and Early Training Projects." *Journal of the American Statistical Association* 103, no. 484 (2008): 1481–95.

Money - Amana Market	Secondary	Survey	Self-reported assessment money is kept safe from fraud when using Amana Market, on a scale of 1 (strongly disagree)-7 (strongly agree)

Recruitment and Sampling

Overall Plan and Sampling Pool

The recruitment process involves two distinct groups: existing users and newly onboarded users within CoAmana. Each group initially aimed to achieve a target sample size of 1,800 individuals. The sampling pool was derived from three key states of operation: Kano, Kaduna, and Jigawa, which represent the primary regions of CoAmana's activities. Table 3 outlines the make-up of the final sample for this study.

Recruitment Plan for Existing Users

To sample existing users for the randomized evaluation,

1. CoAmana utilized its comprehensive user database, which contained essential information such as Name, Contact details, State, Local Government Area (LGA), and Gender.
2. A stratified random sampling technique was employed using statistical software to select participants from the database.
3. To ensure a representative sample, the selection process was stratified based on predetermined expectations regarding state and gender variables. This approach aimed to capture the diversity within the existing user population and mitigate potential biases.
4. During a compliance call, existing users are introduced to the study and invited to participate in the baseline survey.

Recruitment Plan for New Users

To sample new users for the randomized evaluation, CoAmana deployed a team of field representatives to recruit new users to the CoAmana platform. .

1. These representatives engaged with potential users (market leaders and lead agents) in markets and facilitated their onboarding process onto the CoAmana platform.
2. Once consent was obtained from the individuals to trade through CoAmana, they were set up and provided access to the platform.
3. As part of the onboarding process, new users undergo a compliance verification procedure to confirm their existence and details. This verification was primarily conducted through CoAmana's call center.
4. Additionally, during this stage, users are introduced to the study and invited to participate in the baseline survey, which served as a starting point for the evaluation.

Table 3: Sample Selection

New Users				Existing Users		
	Male	Female			Male	Female
Kaduna	25	14		Kaduna	197	481
Kano	1267	209		Kano	447	466
Jigawa	246	38		Jigawa	217	5
	1538	261			880	933

Timeline of randomized evaluation

The timeline for the experiment is as follows. The onboarding took place from May 22nd to July 24th 2023, where a short baseline survey was collected with onboarding. After onboarding, participants were randomized into the treatment and control groups. Experimental manipulation happens in a set of three compliance calls. The first set of compliance calls will begin August 3rd and are scheduled to last until the week of January 8th. The second set of compliance calls starts after this one and lasts until the week of November 5th. Finally the third set of compliance calls lasts until December 31st. After this last set of compliance calls has finished, the endline phone survey will run from the week of January 8th to February 4th 2024.

Study Design and Interventions

Informed by learnings from a recent lab-in-the-field study, the following are the two interventions tested in this field experiment.

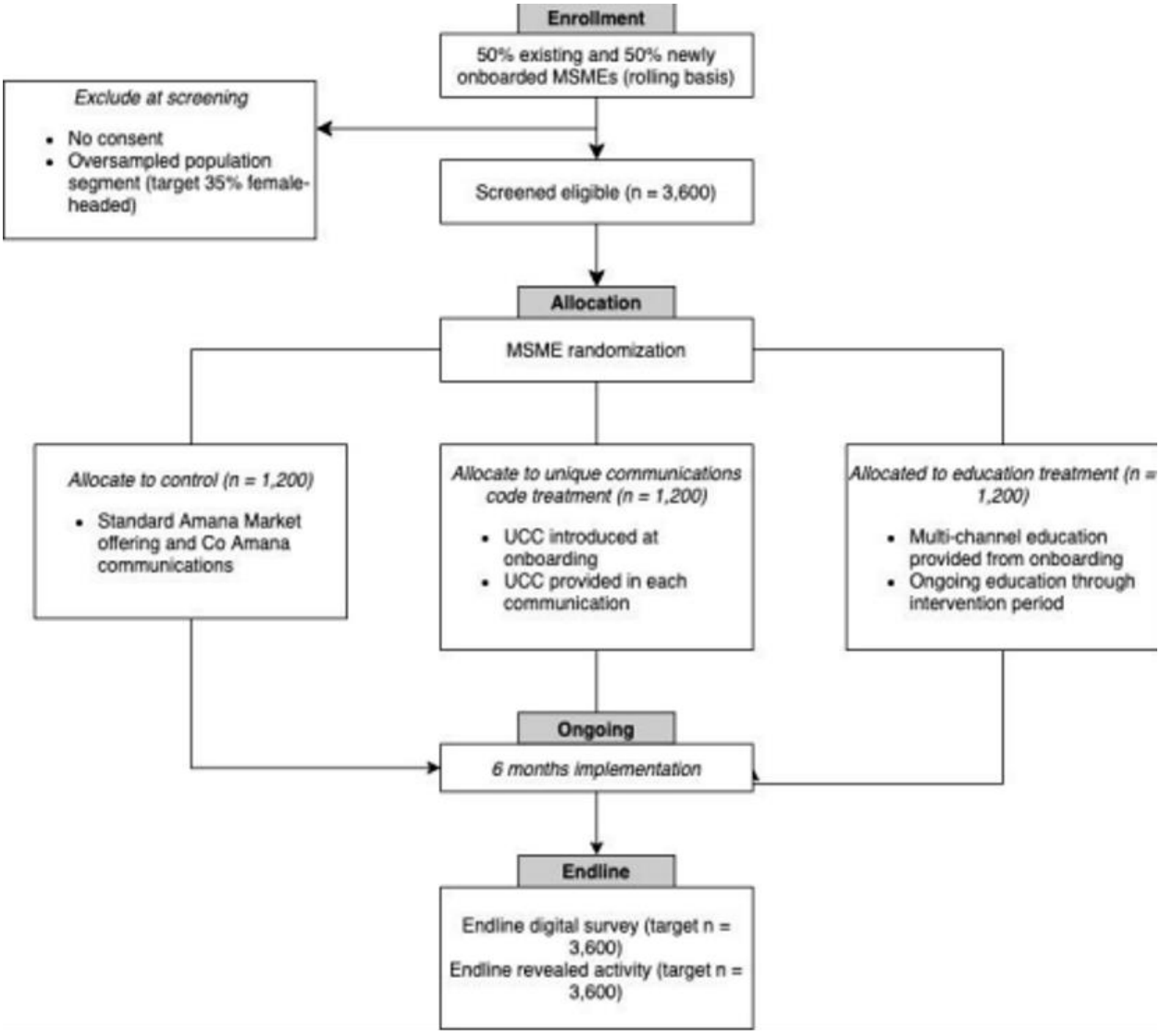
Table 4: Anti-Fraud Interventions

Control	This group will receive the compliance calls as standard procedure.
Treatment 1 (Education)	T1 participants will receive three compliance calls (every two months) which will include information about the five key signs of potential fraud which is narrated in an audio file. This information is prefaced by a general warning message. Participants will listen to an audio recording presenting key warning signs to look out for to identify fraud. To test their understanding of the recording, participants will be presented with 2 fraudulent or genuine communication scenarios and are asked what they would do in each scenario. The call centre agent will explain the correct answers. Immediately after the call participants will receive a follow up SMS summarizing the key warning signs.

Treatment 2 (UCC)	This group will receive the same compliance calls as the treatment and control groups and will be informed about their unique communication codes. They will: ● Be introduced to the UCC system. ● Be assigned a randomly generated and recorded centrally 5-digit UCC code to authenticate future communications with Amana Market. ● Immediately after the call participants will receive a follow up SMS with their unique code to look out for in all future communication from Amana Market.

All participants are randomized into either a control group, an embedded anti-fraud focused financial literacy intervention or the unique communications code (UCC) group as per the design in Figure 1.

Figure 1: Study Outline



Study Hypotheses

This study will explore whether providing MSEs with education about digital fraud affects fraud victimization, their confidence in deciphering fraud, their trust in digital financial services, and their willingness to use digital financial services. These are reflected in detail in hypotheses 1.1-5.6 in table 5. Additionally, we will explore heterogeneity in treatment effects, as reflected in hypotheses 6.1 and 7.1. For all outcomes, we will allow impacts to vary by past experience with financial services, ICTs, and fraud attempts; demographic characteristics; and socio-economic status. For victimization and usage outcomes, we will additionally allow impacts to vary by risk preferences.

Table 5: Research hypotheses for core research questions

Research Question	Number	Hypothesis
Do anti-fraud interventions reduce MSEs susceptibility to fraudulent communications?	1.1	Anti-fraud interventions affect MSE compliance (or engagement) with fraudulent communication. (T1, T2 vs. C)
	1.2	Anti-fraud interventions affect MSE losses from fraud. (T1, T2 vs. C)
	1.3	Anti-fraud interventions affect MSE ability to distinguish between genuine and fraudulent communications. (T1 vs. C)
Do anti-fraud interventions increase confidence in one's ability to distinguish between genuine and fraudulent communications?	2.1	Anti-fraud interventions affect MSE confidence to distinguish between genuine and same fraudulent communications. (T1 vs. C)
Do anti-fraud interventions increase knowledge about types of fraudulent communications?	3.1	Anti-fraud interventions affect MSE knowledge about the signs of fraud. (T1, T2 vs. C)
Do anti-fraud interventions increase usage of digital finance services?	4.1	Anti-fraud interventions affect usage of an online marketplace platform. (T1, T2 vs. C)
	4.2	Anti-fraud interventions have a non-uniform effect on the usage of online marketplace platform over time. (T1, T2 vs. C)
	4.3	Anti-fraud interventions affect the likelihood of the usage of digital financial services. (T1, T2 vs. C)
Do anti-fraud interventions increase trust in digital financial services, and specifically in Amana Market?	5.1	Anti-fraud interventions affect trust in digital financial services. (T1, T2 vs. C)
	5.2	Anti-fraud interventions affect trust in Amana Market. (T1, T2 vs. C)
	5.3	Anti-fraud interventions affect belief that personal information is safe at digital financial services. (T1, T2 vs. C)
	5.4	Anti-fraud interventions affect belief that personal information is safe at Amana Market. (T1, T2 vs. C)
	5.5	Anti-fraud interventions affect belief that money is safe at digital financial services. (T1, T2 vs. C)
	5.6	Anti-fraud interventions affect belief that money is safe at Amana Market. (T1, T2 vs. C)
Does experience with ICTs, DFS, or past fraud attempts serve as a substitute or complement to the anti-fraud interventions?	6.1	Treatment effects depend on prior experience with ICT, DFS and fraud.

Are anti-fraud interventions equally effective for subgroups with different demographic characteristics, socioeconomic status, and preferences?	7.1	Treatment effects depend on gender, age, income, education, and risk aversion.

Balance Checks

We will test that those who are assigned to treatment are not different from those who are assigned to control. We plan to use a joint test of orthogonality to test balance across treatment groups, holding out those variables that we have already stratified treatment upon (e.g., gender, if they were newly recruited to the platform, and state). Additionally, since there are multiple treatment groups within our experiment, we will perform a multinomial logit regression and then test for joint orthogonality of coefficients.

4. Empirical Strategy

Estimation of Treatment Effects

To estimate the causal effect of treatments on survey outcomes we estimate the following empirical specification:

$$Y_i = \alpha + \beta_1 T_{1i} + \beta_2 T_{2i} + \varepsilon_i$$

where we define Y_{is} to be one of the outcome variables described in Table 1 or Table 2 for participant i. β_1 estimates the treatment effect of treatment 1 (education) and β_2 estimates the treatment effect of treatment 2 (UCC).

We use this specification to understand the effect on victimization (compliance or losses), detection, knowledge, self-confidence, as well as self-reported trust and usage outcomes. For usage outcomes using the Amana Market data, we will estimate the effect of treatment on total usage. However, we can also decompose this into intensive and extensive margins. To do so, we run the above specification as a linear probability model to understand the participation effect. Additionally, we will estimate a Tobit model to understand the conditional-on-participation effect.

For each specification, we will perform the following two-sided hypothesis tests after estimation:

- $H_0: \beta_1 = 0$. Providing MSEs with key warning signs impacts knowledge of fraud, detection ability, detection confidence, reduces victimization, and trust and usage of DFS.

- $H_0: \beta_2 = 0$. Providing MSEs with the UCC impacts knowledge of fraud, detection ability, detection confidence, reduces victimization, and trust and usage of DFS.

Robustness: Selection-on-Observables

For robustness, we will re-estimate our hypotheses using a selection-on-observables approach. However, absent clear evidence that randomization has failed along an important dimension, these will not represent preferred estimates. We estimate:

$$Y_i = \alpha + \beta_1 T_{1i} + \beta_2 T_{2i} + \vec{X}_i' \theta + \varepsilon_i$$

where $\vec{X}_i$ is a vector of control variables. In particular, we will control for functions of the factors specified in Table 7: smartphone ownership, formal financial accounts, baseline fraud victimization, age, education, occupation, income, and risk preferences. We specifically omit gender and region since we stratify treatment assignment by gender and by region.

Heterogeneous Treatment Effects

Estimation of Heterogeneous Treatment Effects

To allow for segmentation and analysis of heterogeneity, the survey will additionally collect information relating to attitudinal and behavioural characteristics, as well as relevant demographic factors. We estimate heterogeneous treatment effects by interacting indicator variables constructed from baseline characteristics with treatment status. Formally, we estimate the regression:

$$Y_i = \alpha + \beta_1 T_{1i} + \beta_2 T_{2i} + \beta_3 (X_i \times T_{1i}) + \beta_4 (X_i \times T_{2i}) + \varepsilon_i$$

where X_i is an indicator variable constructed from the baseline characteristic of interest. See Table 7 for the planned construction of these variables. In this case, β_1 and β_3 are the treatment effects of treatment 1 within each of the two subgroups defined by X_i and β_2 and β_4 are the treatment effects of treatment 2 within each of the two subgroups defined by X_i.

Experience with ICTs, Financial Services, and Fraud

Does experience with information communication technologies (ICTs), financial services and fraud serve as a substitute or complement to the anti-fraud campaign? The baseline survey will collect information relating to smartphone ownership, formal financial account holding and baseline fraud victimization. These are designed to proxy for experience with ICTs, financial services and fraud. We will test heterogeneity in effects by low and high experience to understand the effect of the anti-fraud treatments on fraud victimization, knowledge, detection ability, and confidence, trust, and usage in these subgroups.

Demographic Characteristics

We will test heterogeneity in effects by demographic characteristics to understand the effect of the anti-fraud treatments on fraud victimization, knowledge, detection ability, and confidence, trust, and usage in

these subgroups. We expect, for example, that younger users might be less vulnerable to fraud compared to older users.

Socio-Economic Status

The dynamics of fraud vary in a number of ways with respect to socio-economic status, which we proxy for using both income and education. Financial literacy may be more useful for low socio-economic status individuals, but may be more easily absorbed by those with high socio-economic status, who tend to have more schooling. We will test heterogeneity in effects by education and income to understand the effect of the anti-fraud treatments on fraud victimization, knowledge, detection ability, and confidence, trust, and usage in these subgroups.

Risk Preferences

Risk preferences may also moderate the effect of greater knowledge, confidence, or discriminatory ability. We will test heterogeneity in effects by risk preferences to understand the effect of the anti-fraud treatments on fraud victimization and usage in these subgroups

Standard Error Adjustments

Treatment assignment is at the individual level, therefore for outcomes with multiple observations per participant, we will apply cluster robust standard errors at the individual level. For any outcomes with only one observation per treatment unit, we will apply heteroskedasticity robust standard errors.

Multiple Hypothesis Testing

As described in the sections above, we opt to reduce the number of tests in each outcome group as opposed to adjusting for multiple hypothesis testing. Specifically, we test a single outcome for each primary outcome group. Where multiple outcomes are of interest, we will construct a standardized index of the outcomes to serve as the primary outcome for that group as in Anderson (2008).[12] Additionally, where appropriate and for purposes of robustness, we will include family wise error rate (FWER)-adjusted p-values and False Discovery Rate (FDR)-adjusted p-values.

Table 7: Controls, Balance, and Heterogeneity - Variables Collected at Baseline

Variable of interest	**Details**
Smartphone ownership	An indicator variable equal to one if the respondent owns a smartphone, and zero otherwise.
Financial account	An indicator variable equal to one if the respondent has an account at a formal financial institution, and zero otherwise.
Baseline fraud victimization	Respondents will be split into as many as four types, conditional on the underlying data: those who have not been contacted by a scammer,

[12] *Ibid.*

	those who were contacted but did not comply, those who complied but did not suffer losses, and those who complied and suffered losses. For sake of power, we may reduce these categories to as few as two. For example if few people responded or faced losses due to fraud, we will reduce the categories to those who have and have not been contacted by a scammer.
Gender	An indicator variable equal to one if the business owner is a woman, zero otherwise.
Age	An indicator variable for if the business owner is above (or below) the median age.
Occupation	A set of indicator variables (and a left-out group) for the following occupations: ● Agriculture ● Non-Agriculture This will draw on Amana market data.
Education	We collect education information about seven categories, which capture both school type and also level of schooling. We will create a low and high group. We will aim to allocate about half of those who had formal schooling to low schooling and half to high schooling, and allocate informal schooling to the low group.
Income	We ask about weekly take home income from their business after costs have been paid. While the survey discretizes income into four categories we will further reduce to low income and high income aiming to allocate about half of the sample into each group.
Willingness to take risks	An indicator variable equal to one if the respondent reports being willing to take risks, and zero otherwise. We will use responses to the question, "indicate your level of agreement for the following statement: I am a person who takes risks." We split the sample into groups that are more and less willing to take risks, with about half of the sample in each group.
Baseline Trust	Index of trust in DFS outcomes.
Baseline Usage	Self-reported likelihood of using DFS in the future as well as usage of Amana Market from administrative data.
Baseline Confidence	A self-assessment of confidence in identifying fraudulent communications.

5. Fieldwork

Data collection

We will conduct the endline data collection through a phone survey, focusing on respondents' experiences of fraud during the study period, their knowledge of common frauds and techniques used by fraudsters, and their self-reported likelihood of engaging in fraud in general, specifically with Amana Market.

Before starting the endline data collection, we will conduct a 3-day pilot to ensure that the study protocols and survey instruments are fine-tuned for smooth data collection. After the pilot, we will provide enumerator training to familiarize the data collectors with the study protocols, the survey instrument, and Computer Assisted Telephone Interviewing (CATI).

After the training, enumerators will be given a list of phone numbers for each respondent, which will be pre-loaded onto the SurveyCTO Collect App. They will be required to call each provided number for about 60 seconds, one after the other, until someone on the other end answers the phone. The enumerators will then confirm the respondent's identity by asking a set of questions related to their age, gender, name, and place of residence. After confirming the respondent's identity, the enumerator will obtain verbal consent to proceed with the survey.

If a respondent does not answer the call or if their phone is off, the enumerators will make nine more attempts in total distributed across 3 days and within different time blocks before giving up on the respondent. We expect modest attrition levels because the respondents have recently interacted with the implementation partner, Amana Market, over the phone.

The data collection process, excluding the pilot, is expected to take about four weeks. It will be carried out by a maximum of 23 enumerators at a designated location, under the supervision of a research associate and a field manager.

Data management

Data Collection Devices: Enumerators will be provided with IPA tablets and Sim cards for data collection. The tablets will be password-protected and accessible only to IPA staff. SurveyCTO's CATI starter kit will be used for organizing call attempts, and a dialer "plug-in" will automate phone calls to specified numbers.

Data Upload and Storage: At the end of each day, enumerators will upload survey data to SurveyCTO's cloud server. The server will have a project-specific login accessible to dedicated IPA staff. Data will be downloaded into Boxcryptor, a secure cloud storage system. Access to data files in Boxcryptor will be restricted to primary research staff with unique, protected passwords. Passwords will be immediately changed if compromised. Data files will be accessed only for authorized research purposes and shared accordingly, with any loss of confidential information reported to the IRB.

Data Sharing and Anonymization: A second folder on the cloud will store data stripped of personal identifying information to comply with Nigeria's data protection Act. Anonymized data in this folder will

be shared with authorized parties outside the primary research team. Anonymized data will be published with the report as per the open access policy of the Gates foundation. Any data that could potentially identify individuals will not be included in reports, articles, or any other public documents produced during the course of this study.

Quality Control Measures: We will use random audio recordings in the survey for data quality checks. Respondents will be informed about this during the consent process, and the recordings will only be used for quality control. Supervisors will sit through at least one full interview conducted by each enumerator in the team and complete a Surveyor Assessment Form during the first 3-4 days of the survey. Additionally, selected questions will be re-administered to a random sample of respondents for back-checking responses. The Research Associate will perform various checks on the data, including consistency, outliers, logical errors, and missing responses and based on this, they will debrief with the field manager and enumerators, seeking clarifications and issuing instructions for re-interviews if necessary.